(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-17686
(P2017-17686A)
(43)公開日　平成29年1月19日(2017.1.19)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675A	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	
G06F	21/44	(2013.01)	G06F	21/44		

審査請求 未請求　請求項の数 15　ＯＬ　外国語出願　（全 34 頁）

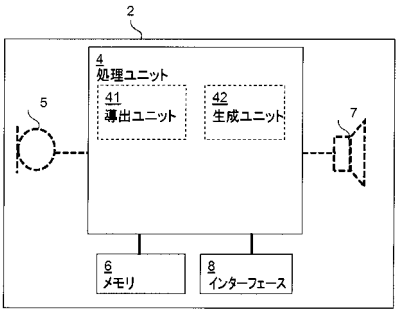
(21)出願番号　特願2016-120155 (P2016-120155)
(22)出願日　平成28年6月16日 (2016.6.16)
(31)優先権主張番号　PA201570437
(32)優先日　平成27年7月2日 (2015.7.2)
(33)優先権主張国　デンマーク (DK)
(31)優先権主張番号　15175141.9
(32)優先日　平成27年7月2日 (2015.7.2)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　503021401
ジーエヌ　リザウンド　エー／エス
ＧＮ　ＲＥＳＯＵＮＤ　Ａ／Ｓ
デンマーク、ディーケー－２７５０　バレラップ、ロートラップジェルグ　７
Ｌａｕｔｒｕｐｂｊｅｒｇ　７，　ＤＫ－２７５０　Ｂａｌｌｅｒｕｐ　Ｄｅｎｍａｒｋ
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　ペダーセン　ブライアン　ダム
デンマーク　４１００　リングステズ　バレッテン　７９

最終頁に続く

(54)【発明の名称】通信ログ機能を備える聴覚デバイスおよび関係する方法

(57)【要約】　（修正有）
【課題】通信ログ機能を備える聴覚デバイスおよび関係する方法を提供する。
【解決手段】聴覚デバイス２は、ユーザの聴力損失を補うように構成された処理ユニット４と、メモリ・ユニット６と、インターフェース８とを備える。また、聴覚デバイス２は、インターフェース８を介してクライアント・デバイスから認証メッセージを受信し、認証メッセージからクライアント・デバイス識別子を導出し、クライアント・デバイス識別子をメモリ・ユニット６に記憶するように構成される。
【選択図】図２



【特許請求の範囲】
【請求項１】
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、
メモリ・ユニットと、
インターフェースとを備える聴覚デバイスであって、
前記インターフェースを介して、クライアント・デバイスから認証メッセージを受信し、
前記認証メッセージからクライアント・デバイス識別子を導出し、
前記メモリ・ユニットに前記クライアント・デバイス識別子を記憶するように構成される
聴覚デバイス。
【請求項２】
前記認証メッセージは、暗号化されたクライアント・デバイス証明書を含み、前記認証メッセージから前記クライアント・デバイス識別子を導出することは、前記暗号化されたクライアント・デバイス証明書を復号することによって前記暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得することと、前記暗号化されたクライアント・デバイス証明書の前記復号されたバージョンから前記クライアント・デバイス識別子を導出することとを含む請求項１に記載の聴覚デバイス。
【請求項３】
前記認証メッセージは、クライアント・デバイス・タイプ識別子を含み、前記処理ユニットは、前記メモリ・ユニットに前記クライアント・デバイス・タイプ識別子を記憶するように構成される請求項１または２に記載の聴覚デバイス。
【請求項４】
前記認証メッセージは、ユーザ識別子を含み、前記処理ユニットは、前記メモリ・ユニットに前記ユーザ識別子を記憶するように構成される請求項１から３のいずれか一項に記載の聴覚デバイス。
【請求項５】
前記聴覚デバイスは、接続要求を受信したことに応答して前記処理ユニットによってセッション識別子を含む接続応答を生成し、前記インターフェースを介して前記接続応答を送信するように構成される請求項１から４のいずれか一項に記載の聴覚デバイス。
【請求項６】
前記聴覚デバイスは、聴覚デバイス鍵に基づいて前記共通秘密を生成するように構成される請求項５に記載の聴覚デバイス。
【請求項７】
前記聴覚デバイスは、前記セッション識別子を前記メモリ・ユニットに記憶するように構成され、前記セッション識別子は、前記メモリ・ユニット内の前記クライアント識別子にリンクされる請求項５または６に記載の聴覚デバイス。
【請求項８】
前記聴覚デバイスは、前記メモリ・ユニットに記憶されている聴覚デバイス証明書を使用して前記認証メッセージを認証するように構成される請求項１から７のいずれか一項に記載の聴覚デバイス。
【請求項９】
聴覚デバイスを運用する方法であって、前記聴覚デバイスは、前記聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、メモリ・ユニットと、インターフェースとを備えており、前記方法は、
前記インターフェースを介して、クライアント・デバイスから認証メッセージを受信するステップと、
前記認証メッセージからクライアント・デバイス識別子を導出するステップと、
前記メモリ・ユニットに前記クライアント・デバイス識別子を記憶するステップとを含む方法。

【請求項１０】
前記認証メッセージは、暗号化されたクライアント・デバイス証明書を含み、前記認証メッセージからクライアント・デバイス識別子を導出するステップは、前記暗号化されたクライアント・デバイス証明書を復号するステップによって前記暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得するステップと、前記クライアント・デバイス証明書の前記復号されたバージョンから前記クライアント・デバイス識別子を導出するステップとを含む請求項９に記載の方法。
【請求項１１】
前記認証メッセージは、クライアント・デバイス・タイプ識別子を含み、前記方法は、前記メモリ・ユニットに前記クライアント・デバイス・タイプ識別子を記憶するステップを含む請求項９または１０に記載の方法。
【請求項１２】
前記認証メッセージは、ユーザ識別子を含み、前記方法は、前記メモリ・ユニットに前記ユーザ識別子を記憶するステップを含む請求項９から１１のいずれか一項に記載の方法。
【請求項１３】
セッション識別子を生成するステップと、接続要求を受信した後に前記セッション識別子を含む接続応答を送信するステップとを含む請求項９から１２のいずれか一項に記載の方法。
【請求項１４】
前記接続応答は、前記聴覚デバイスの聴覚デバイス識別子を含み、前記共通秘密を生成するステップは、前記聴覚デバイス識別子に基づく請求項１３に記載の方法。
【請求項１５】
前記メモリ・ユニットに記憶されている聴覚デバイス証明書を使用して前記認証メッセージを認証するステップを含む請求項９から１４のいずれか一項に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、聴覚デバイスの分野に関し、詳細には、聴覚デバイスのセキュリティに関する。本開示は、通信ログ機能を備える聴覚デバイスおよび関係する方法に関する。
【背景技術】
【０００２】
聴覚デバイスの機能は、次第に高度化してきている。聴覚デバイスと、聴覚デバイス・フィッティング機器、タブレット、スマートフォン、およびリモート・コントローラなどの外部デバイスとの間のワイヤレス通信が発展している。聴覚デバイスのワイヤレス通信インターフェースは、オープン標準ベースのインターフェースを使用する。しかしながら、このことは、セキュリティに関して多くの問題を提起する。聴覚デバイスは、受信したデータを合法的であるとみなし、不正パーティによるメモリへの書き込みまたは変更を許し得る。そのような攻撃があると、その結果、聴覚デバイスの誤動作、またはバッテリ消耗攻撃が引き起こされ得る。
【０００３】
しかしながら、聴覚デバイスは、計算能力、メモリ空間などに関して厳しい制約条件が課せられている非常に小型のデバイスである。市販のセキュリティ・アルゴリズムおよびプロトコルは、聴覚デバイス上ではたやすく機能し得ない。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
通信および／または通信パーティなどの、活動および／またはアクタを監視する機能を備える聴覚デバイスが必要である。
【課題を解決するための手段】

【０００５】
開示されるのは、聴覚デバイスである。聴覚デバイスは、処理ユニットと、メモリ・ユニットと、インターフェースとを備える。聴覚デバイスは、聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットを備え得る。聴覚デバイスは、インターフェースを介してクライアント・デバイスから認証メッセージを受信するように構成され得る。聴覚デバイスは、認証メッセージからクライアント・デバイス識別子を導出するように構成され得る。聴覚デバイスは、クライアント・デバイス識別子をメモリ・ユニットに記憶するように構成され得る。
【０００６】
本開示の利点は、聴覚デバイスが、通信および通信パーティ（例えば、クライアント・デバイス）などの、聴覚デバイス上で起こる活動をログに取る、または記録することができることである。これは、聴覚デバイスが通信パーティを鍵材料および秘密に関連付けることを可能にし、それにより、通信パーティが聴覚デバイスに復帰したときに、認証および鍵導出が高速化され、簡素化された方式で実行され得る。本開示は、同じまたは対応するレベルのセキュリティを維持しながら、復帰するクライアント・デバイスに対する、改善され、簡素化され、高速化された認証および鍵導出を可能にする。
【０００７】
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、メモリ・ユニットと、インターフェースとを備える、聴覚デバイスを運用する方法も開示されている。方法は、インターフェースを介して、クライアント・デバイスから認証メッセージを受信することと、認証メッセージからクライアント・デバイス識別子を導出することとを含む。方法は、メモリ・ユニットにクライアント・デバイス識別子を記憶することを含み得る。
【０００８】
開示されているような方法および装置は、ログ機能を聴覚デバイスに付与する。これは、聴覚デバイスが、聴覚デバイスに関連している１つまたは複数のクライアント・デバイス識別子をログに取る、または記録することを可能にする。このようにして、例えば、同じクライアント・デバイスが、再び、聴覚デバイスに接続したとき、聴覚デバイスは、第１の接続の場合と同じまたは対応するレベルのセキュリティを維持しながら、第１の接続よりも高速で単純な認証および鍵導出を実行することができる。さらに、本開示は、多数の聴覚デバイス、および多数のクライアント・デバイスに対して、スケーラブルなセキュリティ・アーキテクチャを実現する。
【０００９】
上記、および他の特徴ならびに利点は、添付の図面を参照する例示的な実施形態の以下の「発明を実施するための形態」の説明により、当業者にとって容易に理解できるものとなるであろう。
【図面の簡単な説明】
【００１０】
【図１】本開示による例示的なアーキテクチャの概略図である。
【図２】例示的な聴覚デバイスの概略図である。
【図３Ａ】例示的なクライアント・デバイス証明書の概略図である。
【図３Ｂ】例示的な聴覚デバイス証明書の概略図である。
【図４】本開示によるログ機能を備える例示的な聴覚デバイスと、例示的なクライアント・デバイスとの間の例示的な信号図の概略図である。
【図５】例示的な方法のフローチャートの概略図である。
【図６】例示的な信号図の概略図である。
【発明を実施するための形態】
【００１１】
以下では、図面を参照しながら、様々な実施形態について説明する。全体を通して同様の参照番号は、同様の要素を指す。したがって、同様の要素については、それぞれの図面

の説明に関して詳しくは説明しない。図面は、実施形態の説明を容易にすることのみ意図されていることにも留意されたい。これらは、特許請求の範囲に記載された発明の網羅的説明として、または特許請求の範囲に記載された発明の技術的範囲の限定として、意図されていない。さらに、図示されている実施形態は、図示されているすべての態様または利点を有している必要はない。特定の実施形態と併せて説明されている態様または利点は、必ずしもその実施形態に限定されず、そのように図示されていない、またはそのように明示的に説明されていないとしても、他の任意の実施形態で実施され得る。

【００１２】

本明細書全体を通して、同じ参照番号は、同一のまたは対応する部分に対して使用される。

【００１３】

本開示の目的は、当技術分野における上述の欠点および不利点のうちの１つまたは複数を、単独で、または組み合わせて、軽減するか、緩和するか、または排除しようとする、聴覚デバイスおよび聴覚デバイスを製造する方法を提供することである。

【００１４】

本明細書で使用されるとき、「聴覚デバイス」という用語は、聴覚器具、補聴デバイス、ヘッドセット、一組のヘッドフォンなどの、ユーザが音を聴くのを補助するように構成されたデバイスを指す。

【００１５】

本明細書で使用されるとき、「証明書」という用語は、デバイスの素性および内容の正当性および／または真正性を検証することなどの、デバイスの素性および内容の検証を可能にするデータ構造体を指す。証明書は、証明書の発行者によって証明書の保有者に関連付けられている内容を提示するように構成される。証明書は、適宜、１つまたは複数の暗号鍵（例えば、クライアント・デバイス鍵）への識別子／ポインタなどの、鍵材料、および／またはデジタル署名を備えており、したがって、証明書の受領者は、証明書の内容および素性を検証または認証することができる。これにより、証明書は、素性および内容の認証、否認防止、および／または完全性保護を達成することを可能にする。証明書は、有効期間、１つまたは複数のアルゴリズム・パラメータ、および／または発行者をさらに含み得る。証明書は、デジタル証明書、公開鍵証明書、属性証明書、および／または承認証明書を含むものとしてよい。証明書の例として、Ｘ．５０９証明書、およびセキュア／マルチパーパス・インターネット・メール・エクステンション（Ｓ／ＭＩＭＥ）証明書、および／またはトランスポート・レイヤ・セキュリティ（ＴＬＳ）証明書が挙げられる。

【００１６】

本明細書で使用されるとき、「鍵」という用語は、暗号鍵、すなわち、暗号アルゴリズムの機能的出力を決定するデータ（例えば、文字列、パラメータ）を指す。例えば、鍵は、暗号化ではプレーン・テキストから暗号文への変換、および復号ではその逆の変換を行うことを可能にする。鍵は、デジタル署名および／またはメッセージ認証コード、ＭＡＣを検証するためにも使用され得る。鍵は、同じ鍵が暗号化と復号の両方に使用されるとき、いわゆる対称鍵である。非対称暗号法または公開鍵暗号法では、鍵材料は、鍵ペアであり、いわゆる、公開鍵と秘密鍵とを備える秘密／公開鍵ペアである。非対称または公開鍵暗号システム（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｅｌｍａｎ（ＲＳＡ）暗号システムなど）では、公開鍵は、暗号化および／または署名検証に使用され、秘密鍵は、復号および／または署名生成に使用される。聴覚デバイス鍵は、対称セッション鍵を導出することを可能にする鍵材料であるものとしてよい。聴覚デバイス鍵は、例えば、製造時に、聴覚デバイスのメモリ・ユニットに記憶され得る。聴覚デバイス鍵は、対称鍵を導出するために使用される鍵材料を備え得る。聴覚デバイス鍵は、例えば、ＡＥＳ－１２８ビット鍵などの、Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ（ＡＥＳ）鍵を含む。

【００１７】

本明細書で使用されるとき、「識別子」という用語は、分類する、および／または一意に識別するなど、識別するために使用されるデータを指す。識別子は、単語、数、英字、

記号、リスト、アレイ、またはこれらの任意の組合せの形態をとり得る。例えば、数としての識別子は、符号なし整数のアレイなど、長さが例えば８ビット、１６ビット、３２ビットなどの、符号なし整数（ｕｉｎｔ）などの整数の形態をとり得る。鍵識別子は、クライアント・デバイスなどの、外部パーティとの通信を保護するための鍵材料として使用されるべき鍵を示し得る。例えば、聴覚デバイス鍵識別子は、例えば、証明書鍵および／または通信を保護するためのセッション鍵を導出するために現在使用されるべき鍵などの、複数の聴覚デバイス鍵のうちの１つの聴覚デバイス鍵を指す、および／または識別する。

【００１８】

本開示は、聴覚デバイスに関する。聴覚デバイスは、処理ユニットと、メモリ・ユニットと、インターフェースとを備える。聴覚デバイスは、聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットを備え得る。インターフェースは、例えば、２．４から２．５ＧＨｚの範囲内の周波数でワイヤレス通信するように構成された、ワイヤレス・トランシーバを備え得る。１つまたは複数の例示的な聴覚デバイスにおいて、インターフェースは、データを受信し、および／または送信するように構成されたワイヤレス・トランシーバをそれぞれ備える、クライアント・デバイスおよび／または聴覚デバイスと、ワイヤレス通信などの、通信を行うように構成される。処理ユニットは、例えば、受信されたデータに従って聴覚デバイスのユーザの聴力損失を補うように構成され得る。聴覚デバイスは、インターフェースを介して、クライアント・デバイスから認証メッセージを受信するように構成され得る。例えば、インターフェースは、クライアント・デバイスから認証メッセージを受信するように構成され得る。例えば、聴覚デバイスは、通信セッションを確立するためにクライアント・デバイスから認証メッセージを受信する。本明細書で使用されている「クライアント・デバイス」という用語は、聴覚デバイスと通信するデバイスを指す。クライアント・デバイスは、クライアントとして動作するコンピューティング・デバイスを指すものとしてよい。クライアント・デバイスは、フィッティング・デバイス、ハンドヘルド・デバイス、リレー、タブレット、パーソナル・コンピュータ、携帯電話、パーソナル・コンピュータもしくはタブレットまたは携帯電話上で実行されるアプリケーション、および／またはパーソナル・コンピュータにプラグ接続されるＵＳＢドングルを含み得る。クライアント・デバイスは、フィッティング・データ、聴覚デバイス動作パラメータ、および／またはファームウェア・データのいずれかを送信することによって、聴覚デバイスの動作を制御することができる。聴覚デバイスは、認証メッセージからクライアント・デバイス識別子を導出するように構成され得る。クライアント・デバイス識別子は、クライアント・デバイスを識別する識別子を指す。クライアント・デバイス識別子は、例えば、クライアント・デバイスの媒体アクセス制御（ＭＡＣ）アドレス、および／またはクライアント・デバイスのシリアル番号を含み得る。クライアント・デバイス識別子は、例えば、聴覚デバイスが複数のクライアント・デバイスのうちからクライアント・デバイスを識別することを可能にする。聴覚デバイスは、クライアント・デバイス識別子をメモリ・ユニットに記憶するように構成され得る。処理ユニットは、メモリ・ユニットにクライアント・デバイス識別子を記憶し得る。メモリ・ユニットは、限定はしないが、読出し専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、などを含む、取り外し可能なおよび取り外し不可能なデータ記憶ユニットを含み得る。クライアント・デバイス識別子をメモリ・ユニットに記憶することは、ログ機能に寄与し得る、すなわち、聴覚デバイスが、聴覚デバイスに関連している１つまたは複数のクライアント・デバイス識別子をログに取る、または記録することを可能にする。これにより、次の通信またはフィッティング・セッションなど、後の段階で、聴覚デバイスと再接続する同じクライアント・デバイスの鍵導出および認証の簡素化を可能にするという利点がもたらされ得る。

【００１９】

認証メッセージは、暗号化されたクライアント・デバイス証明書を備え得る。クライアント・デバイスは、クライアント・デバイス証明書を割り当てられ得る。クライアント・デバイス証明書は、例えば、クライアント・デバイスを製造するデバイスによって、生成

され、クライアント・デバイスに割り当てられる証明書を指す。暗号化されたクライアント・デバイス証明書は、暗号化アルゴリズムおよび証明書鍵を使用してクライアント・デバイスによって生成され得る。

【００２０】

クライアント・デバイス証明書は、証明書タイプ識別子を備え得る。証明書タイプ識別子は、聴覚デバイス・ファミリ証明書タイプ、聴覚デバイス証明書タイプ、ファームウェア証明書タイプ、研究開発証明書タイプ、クライアント・デバイス証明書タイプなどの、さまざまな証明書タイプのうちの証明書の１つのタイプを示し得る。証明書タイプ識別子は、どのようなタイプの証明書を聴覚デバイスが受信し、記憶し、および／または取り出すかを識別するために聴覚デバイスによって使用され得る。

【００２１】

クライアント・デバイス証明書は、証明書のデータ・フォーマット・バージョンを示すバージョン識別子を含むものとしてよい。聴覚デバイスは、証明書タイプ識別子および／またはバージョン識別子を使用して、証明書がどのようなタイプのデータを含むか、どのようなタイプのデータが証明書のフィールドに入っているかを決定するように構成され得る。例えば、聴覚デバイスは、証明書タイプ識別子および／またはバージョン識別子に基づいて、証明書のどのようなフィールドがデジタル署名を含むか、および／またはデジタル署名を検証するためにどの公開鍵が必要かを決定することができる。証明書タイプ識別子と公開／秘密鍵ペアとの間に一対一マッピングがあることが想定され得る。

【００２２】

クライアント・デバイス証明書は、署名デバイス識別子を備え得る。署名デバイス識別子は、クライアント・デバイス証明書に署名したデバイス（製造デバイス、例えば、集積回路カード、スマート・カード、ハードウェア・セキュリティ・モジュールなど）を識別する一意の識別子を指す。署名デバイス識別子は、例えば、署名デバイスの媒体アクセス制御（ＭＡＣ）アドレス、シリアル番号を含み得る。署名デバイス識別子は、例えば、聴覚デバイスが、署名デバイスが例えばブラックリストに載っているかどうかを決定すること、したがってブラックリストに載っている署名デバイスによって署名された証明書を拒絶することを可能にする。

【００２３】

クライアント・デバイス証明書は、１つまたは複数のハードウェア識別子を備え得る。ハードウェア識別子は、クライアント・デバイスに備えられている無線チップ、クライアント・デバイスのデジタル・シグナル・プロセッサなどの、クライアント・デバイスに備えられているハードウェアを識別することができる。ハードウェア識別子は、ハードウェアの製造時に聴覚デバイスに備えられているハードウェアのレジスタに記憶され得る。ハードウェア識別子は、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組合せを含み得る。

【００２４】

クライアント・デバイス証明書は、クライアント・デバイス・タイプ識別子を備え得る。クライアント・デバイス・タイプ識別子は、クライアント・デバイスが属しているタイプを示し得る。クライアント・デバイスは、フィッティング・タイプ、例えば、聴覚デバイスをフィッティングするように構成されたタブレット製品モデル、カテゴリ、またはタイプ、聴覚デバイスをフィッティングするように構成されたＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアント・デバイスのモデル、カテゴリ、またはタイプに対応するクライアント・デバイス・タイプを割り当てられ得る。

【００２５】

クライアント・デバイス証明書は、クライアント・デバイス識別子を備え得る。クライアント・デバイス証明書は、クライアント・デバイス鍵識別子を備え得る。クライアント・デバイス鍵識別子は、聴覚デバイスなどの、外部パーティとの通信を保護するための鍵材料として使用されるクライアント・デバイス鍵を示し得る。クライアント・デバイス鍵識別子は、どのクライアント・デバイス鍵が、クライアント・デバイス証明書の一部であ

るかを示し得る。１つまたは複数の例示的なクライアント・デバイス証明書において、クライアント・デバイス証明書は、クライアント・デバイスのＢｌｕｅｔｏｏｔｈ（登録商標）アドレスを含む。

【００２６】

クライアント・デバイス証明書は、デジタル署名を備える。デジタル署名は、署名者の正当性の検証などの、聴覚デバイス証明書の真正性の立証または検証を可能にする。デジタル署名は、適宜、クライアント・デバイス・フィッティング秘密鍵を使用して製造デバイスによって生成される。

【００２７】

聴覚デバイスは、デジタル署名を備えるクライアント・デバイス証明書を受信したとき（すなわち、暗号化されたクライアント・デバイス証明書を含む認証メッセージを受信し、クライアント・デバイス証明書の復号されたバージョンを取得したとき）にデジタル署名を検証するように構成され得る。デジタル署名は、対応するクライアント・デバイス・フィッティング公開鍵を使用して聴覚デバイスによって検証可能である。デジタル署名が、申し立てられた公開鍵を使用して検証に成功しなかった場合、聴覚デバイスは、クライアント・デバイス証明書（認証メッセージ）を破棄し、および／または通常動作を中断することができる。これは、聴覚デバイスが改竄されたまたは非認証パーティから受信されたクライアント・デバイス証明書を拒絶するという利点をもたらし得る。したがって、聴覚デバイスとの通信は、偽装攻撃、変更攻撃、およびなりすまし攻撃に対してロバストであり得る。

【００２８】

認証メッセージからクライアント・デバイス識別子を導出することは、暗号化されたクライアント・デバイス証明書を復号することによって暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得することと、暗号化されたクライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出することとを含み得る。聴覚デバイスは、証明書鍵、共通秘密（ｃｏｍｍｏｎ　ｓｅｃｒｅｔ）、および／または聴覚デバイス鍵を使用して、暗号化されているクライアント・デバイス証明書を復号するように構成され得る。証明書鍵は、共通秘密および／または証明書値に基づくものとしてよい。聴覚デバイスは、聴覚デバイス鍵に基づいて共通秘密を生成するように構成され得る。例えば、聴覚デバイス鍵に基づいて共通秘密を生成するために、聴覚デバイスは、メモリ・ユニットから聴覚デバイス証明書またはその一部を取り出し、聴覚デバイス証明書は、共通秘密を導出するために使用される、聴覚デバイス鍵を含む。

【００２９】

聴覚デバイスは、処理ユニットを使用してセッション識別子に基づいて共通秘密を生成し、共通秘密をメモリ・ユニットに記憶するように構成され得る。例えば、聴覚デバイスは、聴覚デバイス鍵およびセッション識別子に基づいて、共通秘密を生成することができる。聴覚デバイスは、共通秘密ＣＳを、例えば以下の式

ＣＳ＝ｈａｓｈ（ＨＤ＿ＫＥＹ，Ｓ＿ＩＤ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＫＥＹは聴覚デバイス鍵であり、Ｓ＿ＩＤはセッション識別子である。聴覚デバイス鍵は、共通秘密として使用され得る。セッション識別子は、接続要求を受信したとき聴覚デバイスによって生成され得る。セッション識別子は、定義された長さの乱数または疑似乱数を含むものとしてよい。共通秘密は、１つまたは複数の例示的な聴覚デバイス内の証明書鍵として使用され得る。

【００３０】

証明書鍵は、共通秘密および／または証明書値に対してハッシュ関数を実行することによって生成され得る。次いで、聴覚デバイスは、証明書鍵Ｃ＿ＫＥＹを、例えば以下の式

Ｃ＿ＫＥＹ＝ｈａｓｈ（ＣＳ，Ｃ＿ＶＡＬ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＣＳは共通秘密であり、Ｃ＿ＶＡＬは証明書値である。証明書値は、予め定義された値または文字列、例えば

「ｃｅｒｔｉｆｉｃａｔｅ」であってよい。

【００３１】

１つまたは複数の例示的な聴覚デバイスにおいて、証明書鍵は、適宜、聴覚デバイス鍵およびセッション識別子に対してハッシュ関数を実行することによって生成され得る。聴覚デバイスは、聴覚デバイスによって生成された／取得された証明書鍵を使用して暗号化されているクライアント・デバイス証明書を復号し、クライアント・デバイス証明書の復号されたバージョンを取得することができる。その後、聴覚デバイスは、クライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出し、クライアント・デバイス識別子を記憶し得る。聴覚デバイスは、クライアント・デバイス証明書の復号されたバージョンの内容を検証し得る。

【００３２】

認証メッセージは、クライアント・デバイス・タイプ識別子を、例えば、（暗号化された）クライアント・デバイス証明書の一部として備え得る。処理ユニットは、メモリ・ユニットにクライアント・デバイス・タイプ識別子を記憶するように構成され得る。クライアント・デバイスは、フィッティング・タイプ、例えば、聴覚デバイスをフィッティングするように構成されたタブレット製品モデル、カテゴリ、またはタイプ、聴覚デバイスをフィッティングするように構成されたＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアント・デバイスのモデル、カテゴリ、またはタイプに対応するクライアント・デバイス・タイプを割り当てられ得る。クライアント・デバイス・タイプ識別子は、クライアント・デバイス・タイプを示す識別子を指すものとしてよい。クライアント・デバイス・タイプ識別子は、クライアント・デバイス・タイプを一意に識別することができる。クライアント・デバイス・タイプ識別子は、クライアント・デバイスが属しているタイプを識別し得る。クライアント・デバイス・タイプ識別子は、クライアント・デバイス証明書に含まれ得る。クライアント・デバイス・タイプ識別子をメモリ・ユニットに記憶することは、ログ機能に寄与し得る、すなわち、聴覚デバイスが、聴覚デバイスによって認証されている１つまたは複数のクライアント・デバイス・タイプ識別子をログに取るか、または記録することを可能にする。これにより、次の通信またはセッションなどの、後の段階で同じクライアント・デバイスの認証を簡素化するという利点がもたらされ得る。

【００３３】

認証メッセージは、ユーザ識別子を、例えば、（暗号化された）クライアント・デバイス証明書の一部として備え得る。処理ユニットは、メモリ・ユニットにユーザ識別子を記憶するように構成され得る。ユーザ識別子は、聴覚デバイスに接続するクライアント・デバイスのユーザの識別子を指すものとしてよい。ユーザ識別子は、フィッティング・デバイスを使用して聴覚デバイスに接続するオーディオロジストなどの、クライアント・デバイスのユーザを一意に識別し得る。ユーザ識別子は、クライアント・デバイス製造者および／または聴覚デバイス製造者によって割り当てられ得る。ユーザ識別子は、ユーザ資格証明書にリンクするか、または関連付けられ得る。ユーザ識別子は、暗号化されたクライアント・デバイス証明書の一部として提供され得る。

【００３４】

クライアント証明書は、ユーザ識別子を備え得る。ユーザ識別子をメモリ・ユニットに記憶することは、ログ機能に寄与し得る、すなわち、聴覚デバイスが、聴覚デバイスによって認証され、聴覚デバイスへのアクセスが正常に得られた１つまたは複数のユーザ識別子をログに取る、または記録することを可能にする。これにより、次の通信などの、後の段階で同じユーザおよびクライアント・デバイスの鍵導出および認証を簡素化するという利点がもたらされ得る。

【００３５】

聴覚デバイスは、処理ユニットによって、接続要求の受信に応答してセッション識別子を含む接続応答を生成するように構成され得る。聴覚デバイスは、インターフェースを介して、接続応答を送信するように構成され得る。聴覚デバイスは、例えばクライアント・

デバイスから接続要求を受信するように構成され得る。接続要求を受信した後、聴覚デバイスは、乱数または疑似乱数を生成することによってセッション識別子を生成するように構成され得る。例えば、聴覚デバイスは、接続要求を受信し、セッション識別子（例えば、乱数）を生成し、クライアント・デバイスへの接続応答にセッション識別子を含めるように構成され得る。

【００３６】

聴覚デバイスは、処理ユニットによって、セッション識別子に基づいて共通秘密を生成し、および／または共通秘密をメモリ・ユニットに記憶するように構成され得る。共通秘密に関係する説明に関連して示されているように、共通秘密は、聴覚デバイス鍵および／またはセッション識別子に基づいて生成され得る。共通秘密をメモリ・ユニットに記憶することは、ログ機能に寄与し得る、すなわち、聴覚デバイスが、１つまたは複数の共通秘密をログに取り、または記録し、それにより記憶されている共通秘密から直接クライアント・デバイスに対する証明書鍵を導出することを可能にする。これは、同じクライアント・デバイスについて、共通秘密を再計算しなくて済むようにする。さらに、共通秘密を記憶することで、トークンベースの認証を可能にし得る。聴覚デバイスは、共通秘密をクライアント・デバイス識別子にリンクするように構成され得る。共通秘密をクライアント・デバイス識別子にリンクすることは、テーブルにおいて共通秘密をクライアント・デバイス識別子に関連付けることを含み得る。共通秘密をクライアント・デバイス識別子にリンクすることで、同じクライアント・デバイスが聴覚デバイスに再接続し、認証メッセージにおいてプレーン・テキストでそのクライアント・デバイス識別子を提供するとき、聴覚デバイスがメモリから共通秘密を取り出し、共通秘密に基づいて直接証明書鍵を導出することを可能にし得る。これは、聴覚デバイスに対してある程度の計算効率をもたらし、それにより、聴覚デバイスの電力効率のよい動作を実現し得る。

【００３７】

聴覚デバイスは、メモリ・ユニットにセッション識別子を記憶するように構成され得る。セッション識別子は、メモリ・ユニット内のクライアント識別子にリンクされ得る。セッション識別子をメモリ・ユニットに記憶することは、ログ機能に寄与し得る、すなわち、聴覚デバイスが、将来の通信のために１つまたは複数のセッション識別子をログに取る、または記録することを可能にする。聴覚デバイスは、セッション識別子とクライアント識別子との間のメモリ関連付けを実行するなど、またテーブルにおいて、共通秘密をクライアント・デバイス識別子に関連付けるなどのために、メモリ・ユニットにおいてセッション識別子およびクライアント識別子をリンクするように構成され得る。これにより、次の通信またはセッションなどの、後の段階で同じユーザおよびクライアント・デバイスの認証を簡素化するという利点がもたらされ得る。

【００３８】

聴覚デバイスは、メモリ・ユニットに記憶されている聴覚デバイス証明書を使用して認証メッセージを認証するように構成され得る。例えば、聴覚デバイスは、認証メッセージの内容、発信元、および／または完全性を検証することによって認証メッセージを認証するように構成され得る。認証メッセージは、認証タイプ識別子、および／または認証鍵識別子を含むものとしてよい。認証タイプ識別子は、クライアント・デバイス・タイプ識別子を示し得る。認証鍵識別子は、聴覚デバイス鍵識別子を示し得る。例えば、認証メッセージは、認証タイプ識別子、および／または認証鍵識別子をプレーン・テキストで含むものとしてよい。メモリ・ユニットは、そこに記憶される聴覚デバイス証明書を有するものとしてよい。聴覚デバイス証明書を使用して認証メッセージを認証することは、認証タイプ識別子、および／または認証鍵識別子を検証することを含むものとしてよい。例えば、聴覚デバイスは、認証鍵識別子が聴覚デバイス証明書に含まれる対応する聴覚デバイス鍵識別子と一致することを検証するように構成され得る。例えば、聴覚デバイスは、認証鍵識別子が聴覚デバイス証明書に含まれる対応する聴覚デバイス鍵識別子の値に等しいか、または高い値を有することを検証するように構成され得る。例えば、聴覚デバイスは、認証鍵識別子がクライアント・デバイス証明書の復号されたバージョンに含まれる対応する

クライアント・デバイス鍵識別子と一致することを検証するように構成され得る。例えば、聴覚デバイスは、認証タイプ識別子がクライアント・デバイス証明書の復号されたバージョンに含まれる対応するクライアント・デバイス・タイプ識別子と一致することを検証するように構成され得る。

【００３９】

聴覚デバイス証明書は、聴覚デバイス識別子、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子、および１つまたは複数の聴覚デバイス鍵を備え得る。聴覚デバイス識別子は、聴覚デバイスの一意の識別子を指すものとしてよい。聴覚デバイス鍵識別子は、クライアント・デバイスなどの、外部パーティとの通信を保護するための鍵材料として使用されるべき聴覚デバイス鍵を示し得る。聴覚デバイス鍵識別子は、どの聴覚デバイス鍵が、聴覚デバイス証明書の一部であるかを示し得る。例えば、値「５」を有する第１の聴覚デバイス鍵識別子は、聴覚デバイス証明書が識別子「５」を備える第１の聴覚デバイス鍵を含むことを示しており、場合によっては、証明書中の聴覚デバイス鍵の数に応じて、識別子「６」、「７」、「８」などを備える聴覚デバイス鍵など、識別子が増分することもある。例えば、聴覚デバイス鍵識別子は、複数の聴覚デバイス鍵のうちの１つの聴覚デバイス鍵を指し、および／または識別する。

【００４０】

聴覚デバイス証明書は、複数の聴覚デバイス鍵などの、１つまたは複数の聴覚デバイス鍵を備える。複数の聴覚デバイス鍵は、聴覚デバイス鍵の第１のセットおよび／または第２のセットなどの、聴覚デバイス鍵の１つまたは複数のセットを含み得る。聴覚デバイス鍵のセットは、一次聴覚デバイス鍵を含む１つまたは複数の聴覚デバイス鍵を含む。聴覚デバイス鍵のセットは、二次聴覚デバイス鍵、三次聴覚デバイス鍵、および／または四次聴覚デバイス鍵を含み得る。第１のセットおよび／または第２のセットなどの、聴覚デバイス鍵のセットは、多数の異なる聴覚デバイス鍵を含むか、または多数の異なる聴覚デバイス鍵から成るものとしてよい。聴覚デバイス鍵のセットの中の聴覚デバイス鍵の数は、３から１０の範囲内など、少なくとも３であり得る。３から６個の聴覚デバイス鍵から成る聴覚デバイス鍵のセットは、メモリ・サイズが限られており、聴覚デバイス証明書の面倒で時間のかかる更新を必要とすることなく聴覚デバイスの将来の動作を可能にするうえで十分な聴覚デバイス鍵を提供したい場合に、有利であり得る。複数の聴覚デバイス鍵は、聴覚デバイスが異なる聴覚デバイス鍵を使用して複数のクライアント・デバイスと安全に通信することを可能にする。代替的に、またはそれに加えて、聴覚デバイスは、例えば、現在使用されている聴覚デバイス鍵に従って通信するように構成されているクライアント・デバイスに障害が生じた場合に、別の聴覚デバイス鍵に切り替える、例えば、一次聴覚デバイス鍵から第２の聴覚デバイス鍵に切り替えることができる。１つまたは複数の例示的な聴覚デバイスにおいて、複数の聴覚デバイス鍵は、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを含む。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第１のセットのうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を含む。聴覚デバイス鍵の第１のセットは、第１のクライアント・デバイス・タイプなどの、第１のクライアント・デバイスとの間の通信を保護することのみを目的とする、聴覚デバイス鍵のセット、例えば、３または４つの聴覚デバイス鍵を含み得る。例えば、聴覚デバイス鍵の第１のセットは、第１のクライアント・デバイスによる聴覚デバイス・データの通信を保護するための聴覚デバイス鍵のセットであってよい。

【００４１】

聴覚デバイス証明書は、１つまたは複数のクライアント・デバイス・タイプ承認識別子を備え得る。クライアント・デバイス・タイプは、タブレット製品モデル、カテゴリ、またはタイプ、ＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアント・デバイスのモデル、カテゴリ、またはタイプを含み得る。クライアント・デバイス・タイプ承認識別子は、フィッティングなどのために、聴覚デバイスが通信を承認し得る、または受け入れ得るクライアント・デバイス・タイプの識別子などの、承認されたクライアント・デバイス・タイプの識別子である。例えば、クライアント・デバイス・タイプ承認

識別子は、１つまたは複数も聴覚デバイスにおいて、フィッティングのために聴覚デバイスが許容すべきであるクライアント・デバイスのタイプを示すビット・フィールドである。

【００４２】

聴覚デバイス証明書は、トークン・パラメータを備え得る。トークン・パラメータは、聴覚デバイスとクライアント・デバイスとの間のトークンベースの認証が有効化されているかどうかを示し得る。例えば、トークン・パラメータが、０に設定されている場合、クライアント・デバイスのトークンベースの認証は、聴覚デバイスによって有効化されることはなく、聴覚デバイスは、例えば、クライアント・デバイス・タイプ識別子および／またはクライアント・デバイス識別子（シリアル番号など）の組合せを使用してクライアント・デバイスの認証を実行することになる。例えば、トークン・パラメータが、１に設定されている場合、クライアント・デバイスのトークンベースの認証は、聴覚デバイスによって有効化されることになる、すなわち、聴覚デバイスは、クライアント・デバイスから受信されたトークンに基づいてクライアント・デバイスを認証する。聴覚デバイスは、例えばユーザの介入なくクライアント・デバイスへの接続を受け入れるために使用される受信されたトークン・パラメータに基づいてセッション特有のトークンも導出し得る。

【００４３】

本開示は、聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニット、メモリ・ユニット、およびインターフェースを備える聴覚デバイスを運用する方法に関する。方法は、インターフェースを介して、クライアント・デバイスから認証メッセージを受信することと、認証メッセージからクライアント・デバイス識別子を導出することとを含む。例えば、インターフェースは、クライアント・デバイスから認証メッセージを受信するように構成され得る。クライアント・デバイスは、聴覚デバイスとのセッションまたは接続を開くために、例えば、フィッティング・データ、聴覚デバイス動作パラメータ、および／またはファームウェア・データを送信するために、認証メッセージを聴覚デバイスに送信することができる。クライアント・デバイス識別子を認証メッセージから導出することは、認証メッセージのペイロードを処理することからクライアント・デバイス識別子を取得するなどの、認証メッセージからクライアント・デバイス識別子を取得することを含み得る。方法は、メモリ・ユニットにクライアント・デバイス識別子を記憶することを含み得る。クライアント・デバイス識別子をメモリ・ユニットに記憶することは、ログ機能に寄与し得る。これは、聴覚デバイスが、聴覚デバイスに関連している１つまたは複数のクライアント・デバイス識別子をログに取るか、または記録することを可能にする。

【００４４】

１つまたは複数の例示的な方法において、認証メッセージは、暗号化されたクライアント・デバイス証明書を含む。暗号化されたクライアント・デバイス証明書は、暗号化アルゴリズムおよび証明書鍵を使用してクライアント・デバイスによって生成され得る。

【００４５】

１つまたは複数の例示的な方法において、認証メッセージからクライアント・デバイス識別子を導出することは、暗号化されたクライアント・デバイス証明書を復号することによって暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得することと、クライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出することとを含み得る。暗号化されたクライアント・デバイス証明書を復号することは、暗号化されたクライアント・デバイス証明書を、証明書鍵を使用して復号することを含み得る。証明書鍵は、共通秘密および／または証明書値に基づくものとしてよい。方法は、聴覚デバイス識別子および／または聴覚デバイス鍵に基づいて共通秘密を生成することを含み得る。例えば、暗号化されたクライアント・デバイス証明書を復号することは、聴覚デバイス証明書またはその一部をメモリ・ユニットから取り出すことを含むものとしてよく、聴覚デバイス証明書は聴覚デバイス鍵を含む。例えば、暗号化されたクライアント・デバイス証明書を復号することは、共通秘密に基づいて証明書鍵を生成することを含み得る。例えば、共通秘密を生成することは、聴覚デバイス鍵および／または

セッション識別子に基づいてもよい。方法は、処理ユニットを使用して共通秘密を生成することと、共通秘密をメモリ・ユニットに記憶することとを含み得る。セッション識別子は、接続要求を受信した後に聴覚デバイスによって生成され得る。セッション識別子は、定義された長さの乱数または疑似乱数を含むものとしてよい。共通秘密ＣＳは、例えば以下の式

ＣＳ＝ｈａｓｈ（ＨＤ＿ＫＥＹ，Ｓ＿ＩＤ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＫＥＹは聴覚デバイス鍵であり、Ｓ＿ＩＤはセッション識別子である。

【００４６】

証明書鍵は、共通秘密および／または証明書値に対してハッシュ関数を実行することによって生成することができる。証明書鍵Ｃ＿ＫＥＹは、例えば以下の式

Ｃ＿ＫＥＹ＝ｈａｓｈ（ＣＳ，Ｃ＿ＶＡＬ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＣＳは共通秘密であり、Ｃ＿ＶＡＬは証明書値である。証明書値は、予め定義された値または文字列、例えば「ｃｅｒｔｉｆｉｃａｔｅ」であってよい。

【００４７】

暗号化されているクライアント・デバイス証明書を復号することは、聴覚デバイスによって生成された証明書鍵を使用することに基づくものとしてよく、その結果、クライアント・デバイス証明書の復号されたバージョンを取得し得る。聴覚デバイスは、クライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出し、クライアント・デバイス識別子を記憶し得る。聴覚デバイスは、クライアント・デバイス証明書の復号されたバージョンの内容を検証し得る。

【００４８】

１つまたは複数の例示的な方法において、認証メッセージは、クライアント・デバイス・タイプ識別子を、例えば、（暗号化された）クライアント・デバイス証明書の一部として備える。方法は、メモリ・ユニットにクライアント・デバイス・タイプ識別子を記憶することを含み得る。

【００４９】

１つまたは複数の例示的な方法において、認証メッセージは、ユーザ識別子を含み、方法は、メモリ・ユニットにユーザ識別子を記憶することを含む。ユーザ識別子をメモリに記憶することは、オフライン・フィッティングが必要であるか、または望ましい状況において有益である。

【００５０】

１つまたは複数の例示的な方法において、方法は、接続要求を受信した後にセッション識別子を含む接続応答を、例えば聴覚デバイスにおいて生成し、例えばインターフェースを介して送信する、ことを含む。方法は、ワイヤレス通信インターフェース、起動ボタン、ユーザ入力の検出、および／またはドッキング・イベントなど、インターフェースを介して、接続要求を受信することを含み得る。方法は、セッション識別子として使用されるべき乱数または疑似乱数を生成することなど、セッション識別子を生成することを含み得る。方法は、接続応答を、インターフェースを介して例えばクライアント・デバイスに送信することを含み得る。

【００５１】

方法は、セッション識別子に基づいて共通秘密を生成することと、適宜、共通秘密をメモリ・ユニットに記憶することとを含むものとしてよく、共通秘密はクライアント・デバイス識別子にリンクされている。セッション識別子に基づいて共通秘密を生成することは、ハッシュ関数をセッション識別子および聴覚デバイス鍵に適用することに基づくなど、セッション識別子およびハッシュ関数に基づいて共通秘密を生成することを含み得る。共通秘密を生成することは、例えば認証メッセージの認証タイプ識別子および／または認証鍵識別子に基づいてメモリ・ユニットから聴覚デバイス鍵を取り出すことを含み得る。方法は、共通秘密をクライアント・デバイス識別子にリンクすることを含み得る。例えば、

共通秘密をクライアント・デバイス識別子にリンクすることは、共通秘密をメモリ・ユニット内のテーブルなどの中のクライアント・デバイス識別子に関連付けることを含む。

【００５２】

１つまたは複数の例示的な方法において、接続応答は、聴覚デバイスの聴覚デバイス識別子を含み、共通秘密を生成することは、聴覚デバイス鍵に基づく。例えば、共通秘密を生成することは、メモリ・ユニットに記憶されている聴覚デバイス証明書からなど、メモリ・ユニットから聴覚デバイス鍵を取り出すことを含む。

【００５３】

方法は、セッション識別子をメモリ・ユニットに記憶することと、セッション識別子をメモリ・ユニット内のクライアント・デバイス識別子にリンクすることとを含み得る。セッション識別子をクライアント・デバイス識別子にリンクすることは、セッション識別子を、メモリ・ユニット内のテーブルなどの中の、クライアント・デバイス識別子に関連付けることを含み得る。

【００５４】

１つまたは複数の例示的な方法において、クライアント・デバイス識別子は、セッション識別子および／または共通秘密にリンクされるか、または関連付けられる。

【００５５】

１つまたは複数の例示的な方法において、方法は、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密にリンクすることを含む。例えば、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密にリンクすることは、メモリ・ユニット内の１つまたは複数のテーブルなどの中で、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密に関連付けることを含む。

【００５６】

１つまたは複数の例示的な方法において、方法は、クライアント・デバイス識別子、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密にリンクすることを含む。例えば、クライアント・デバイス識別子、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密にリンクすることは、メモリ・ユニット内の１つまたは複数のテーブルなどの中で、クライアント・デバイス識別子、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子をセッション識別子および／または共通秘密に関連付けることを含む。

【００５７】

方法は、メモリ・ユニットに記憶される聴覚デバイス証明書を使用して認証メッセージを認証することを含み得る。認証メッセージは、認証タイプ識別子、および／または認証鍵識別子を含むものとしてよい。認証タイプ識別子は、クライアント・デバイス・タイプ識別子を示し得る。認証鍵識別子は、聴覚デバイス鍵識別子を示し得る。例えば、認証メッセージは、認証タイプ識別子、および／または認証鍵識別子をプレーン・テキストで含むものとしてよい。メモリ・ユニットは、そこに記憶される聴覚デバイス証明書を有するものとしてよい。聴覚デバイス証明書を使用して認証メッセージを認証することは、認証タイプ識別子、および／または認証鍵識別子を検証することを含むものとしてよい。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子が聴覚デバイス証明書内の聴覚デバイス鍵を示すことを検証することを含み得る。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子が、聴覚デバイス証明書に含まれる対応する聴覚デバイス鍵識別子の値に等しいか、または高い値を有することを検証することを含み得る。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子がクライアント・デバイス証明書の復号されたバージョンに含まれる対応するクライアント・デバイス鍵識別子と一致することを検証することを含む。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、

認証タイプ識別子がクライアント・デバイス証明書の復号されたバージョンに含まれる対応するクライアント・デバイス・タイプ識別子と一致することを検証することを含む。

【００５８】

図１は、聴覚デバイス２の製造、保守、および／または運用に使用され得る例示的なデバイスを概略的に示している。図１は、例示的なシステム１および聴覚デバイス２を示している。システム１は、聴力損失補償に関連して聴覚デバイス２を製造し、保守し、および／または運用するための（例えば、聴覚デバイスをフィッティングするための、または聴覚デバイス・パラメータを更新するための）、１つまたは複数の製造デバイス１２、クライアント・デバイス１０、およびサーバ・デバイス１６を備え得る。

【００５９】

製造デバイス１２は、聴覚デバイスを製造する方法のステップを実行するように構成され得る。製造デバイス１２は、聴覚デバイス識別子と生成された少なくとも１つの聴覚デバイス鍵とを含む聴覚デバイス証明書を生成するように構成され得る。製造デバイス１２は、聴覚デバイス証明書を聴覚デバイスに送信するように構成され得る。製造デバイス１２は、処理要素（プロセッサおよびメモリなどの）を備えることができる。

【００６０】

聴覚デバイス２は、聴覚デバイス２のユーザの聴力損失を補うように構成され得る。聴覚デバイス２は、例えば、一方向または双方向通信リンクなどの通信リンク２３を使用して製造デバイス１２と通信するように構成され得る。通信リンク２３は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２３は、シングルホップ通信リンクまたはマルチホップ通信リンクであってよい。ワイヤレス通信リンクは、Ｂｌｕｅｔｏｏｔｈ、Ｂｌｕｅｔｏｏｔｈ Ｌｏｗ Ｅｎｅｒｇｙ、ＩＥＥＥ ８０２．１１、Ｚｉｇｂｅｅ（登録商標）などの、短距離通信システムを介して実現され得る。聴覚デバイスは、インターフェース８を介してクライアント・デバイス１０から認証メッセージを受信するように構成される。例えば、インターフェース８は、クライアント・デバイス１０から認証メッセージを受信するように構成される。例えば、聴覚デバイス２は、通信セッションを確立するためにクライアント・デバイス１０から認証メッセージを受信する。聴覚デバイス２は、双方向通信リンクなどの通信リンク２１を介してクライアント・デバイス１０に接続するように構成され得る。通信リンク２１は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２１は、シングルホップ通信リンクまたはマルチホップ通信リンクであってよい。ワイヤレス通信リンクは、Ｂｌｕｅｔｏｏｔｈ、Ｂｌｕｅｔｏｏｔｈ Ｌｏｗ Ｅｎｅｒｇｙ、ＩＥＥＥ ８０２．１１、Ｚｉｇｂｅｅなどの、短距離通信システムを介して実現され得る。聴覚デバイス２は、ネットワーク上でクライアント・デバイス１０に接続するように構成され得る。クライアント・デバイス１０は、ディスペンサがユーザのクライアント・デバイス１０を介して聴覚デバイスに接続する補聴デバイスのリモート・フィッティングを可能にし得る。クライアント・デバイス１０は、フィッティング・デバイス１４などのクライアント（例えば、ハンドヘルド・デバイス、リレー、タブレット、パーソナル・コンピュータ、携帯電話、および／またはパーソナル・コンピュータにプラグ接続されるＵＳＢドングル）として動作するコンピューティング・デバイスを含み得る。聴覚デバイス２は、認証メッセージからクライアント・デバイス識別子を導出するように構成される。聴覚デバイスは、クライアント・デバイス識別子をメモリ・ユニットに記憶するように構成され得る。

【００６１】

クライアント・デバイス１０は、双方向通信リンクなどの通信リンク２４を介してサーバ・デバイス１６と通信するように構成され得る。通信リンク２４は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２４は、インターネットなどのネットワークを含み得る。クライアント・デバイス１０は、保守および更新を目的としてサーバ・デバイス１６と通信するように構成され得る。サーバ・デバイス１６は、サーバとして動作する、すなわち、クライアント・デバイス１０および／または聴覚デバイス２からの要求を処理するように構成されたコンピューティング・デバイスを含み得る。サー

バ・デバイス１６は、聴覚デバイス製造者によって制御され得る。サーバ・デバイス１６は、製造、保守および／または運用目的のために通信リンク２２を介して製造デバイス１２と通信するように構成され得る。サーバ・デバイス１６および製造デバイス１２は、同一の場所に置かれる、および／または聴覚デバイス２の製造、保守、および／または運用目的のために１つのエンティティを形成し得る。

【００６２】

図２は、例示的な聴覚デバイス２を概略的に示す。聴覚デバイス２は、処理ユニット４と、メモリ・ユニット６と、インターフェース８とを備える。聴覚デバイス２は、聴覚デバイス２のユーザの聴力損失を補うように構成された処理ユニット４を備える。インターフェース８は、例えば、２．４から２．５ＧＨｚの範囲内の周波数でワイヤレス通信するように構成された、ワイヤレス・トランシーバを備える。インターフェース８は、製造デバイス１２と、有線および／またはワイヤレス通信などの通信を行うように構成される。処理ユニット４は、聴覚デバイスの製造中および／または製造後に受信されたデータに従って補聴器のユーザの聴力損失を補うように構成され得る。聴覚デバイス２は、音声信号を受信し、音声信号を変換済み音声信号に変換するためにマイクロフォン５または複数のマイクロフォンを備える。変換済み音声信号は、音声信号の電気的および／またはデジタル・バージョンであってよい。処理ユニット４は、変換済み音声信号を受信し、聴覚デバイス２のユーザの聴力損失に応じて変換済み音声信号を処理済み音声信号に処理するように構成される。処理済み音声信号は、圧縮され、および／または増幅され、または同様の処理がなされ得る。聴覚デバイス２は、レシーバと称される、出力トランスデューサ／ラウドスピーカ７を備える。レシーバ７は、処理済み音声信号を受信し、それをユーザの鼓膜で受けることができる出力音声信号に変換するように構成される。

【００６３】

聴覚デバイスは、インターフェース８を介してクライアント・デバイス１０から認証メッセージを受信するように構成される。例えば、インターフェース８は、クライアント・デバイス１０から認証メッセージを受信するように構成される。例えば、聴覚デバイス２は、通信セッションを確立するためにクライアント・デバイス１０から認証メッセージを受信する。聴覚デバイス２は、認証メッセージからクライアント・デバイス識別子を導出するように構成される。クライアント・デバイス識別子は、クライアント・デバイス１０を識別する一意の識別子を指す。クライアント・デバイス識別子は、例えば、クライアント・デバイス１０の媒体アクセス制御（ＭＡＣ）アドレス、および／またはクライアント・デバイス１０のシリアル番号を含み得る。クライアント・デバイス識別子は、例えば、聴覚デバイス２が複数のクライアント・デバイス１０のうちからクライアント・デバイス１０を識別することを可能にする。処理ユニット４は、認証メッセージからクライアント・デバイス識別子を導出するように構成され得る。したがって、処理ユニット４は、例えば、導出ユニット４１を備える。聴覚デバイス２は、クライアント・デバイス識別子をメモリ・ユニット６に記憶するように構成され得る。処理ユニット４は、メモリ・ユニット６にクライアント・デバイス識別子を記憶し得る。メモリ・ユニット６は、限定はしないが、読出し専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、などを含む、取り外し可能なおよび取り外し不可能なデータ記憶ユニットを含み得る。クライアント・デバイス識別子をメモリ・ユニット６に記憶することで、次の通信またはフィッティング・セッションなど、後の段階で、聴覚デバイスと同じクライアント・デバイスが再接続する際の鍵の導出および認証の簡素化を可能にするという利点がもたらされ得る。

【００６４】

聴覚デバイス２は、例えばインターフェース８を介して、聴覚デバイス証明書１００を受信するように構成され得る。聴覚デバイス２は、聴覚デバイス証明書を、例えばメモリ・ユニット６に記憶するように構成され得る。聴覚デバイス２は、製造デバイス１２へのアクセスを認めることもでき、製造デバイス１２は次いで聴覚デバイス証明書をメモリ・ユニット６に記憶するか、または書き込む。メモリ・ユニット６は、限定はしないが、読出し専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、などを含む、取り

外し可能なおよび取り外し不可能なデータ記憶ユニットを含み得る。メモリ・ユニット６は、そこに記憶される聴覚デバイス証明書を有するものとしてよい。聴覚デバイス証明書は、聴覚デバイス識別子、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子、および複数の聴覚デバイス鍵を備え得る。メモリ・ユニット６は、メモリ・ユニット６のメモリ・アドレスに記憶されている聴覚デバイス証明書１００を有するものとしてよい。メモリ・ユニット６は、例えば、聴覚デバイス識別子、少なくとも１つの聴覚デバイス鍵識別子、複数の聴覚デバイス鍵、および／または聴覚デバイス証明書に含まれる任意のデータをメモリ・ユニット６の明確に区別できるそれぞれのメモリ・アドレスに記憶しているものとしてよい。聴覚デバイス２は、聴覚デバイス識別子、少なくとも１つの聴覚デバイス鍵識別子、複数の聴覚デバイス鍵、および／または聴覚デバイス証明書に含まれる任意のデータをメモリ・ユニット６の明確に区別できるそれぞれのメモリ・アドレスから取り出すように構成され得る。聴覚デバイス２は、聴覚デバイス証明書またはその少なくとも一部を使用して、クライアント・デバイス、サーバ・デバイス、別の聴覚デバイスなどの、外部エンティティとの通信を保護することができる。

【００６５】

認証メッセージは、暗号化されたクライアント・デバイス証明書を含み得る。認証メッセージは、クライアント・デバイス識別子を、例えば、暗号化されたクライアント・デバイス証明書の一部として備える。インターフェース８は、暗号化されたクライアント・デバイス証明書を含み得る認証メッセージを受信する。１つまたは複数の例示的な聴覚デバイスにおいて、認証メッセージからクライアント・デバイス識別子を導出するために、聴覚デバイス２または処理ユニット６は、暗号化されたクライアント・デバイス証明書を復号することによって暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得し、暗号化されたクライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出する。例えば、処理ユニット６は、証明書鍵を使用して暗号化されたクライアント・デバイス証明書を復号する。証明書鍵は、共通秘密および／または証明書値に基づくものとしてよい。例えば、聴覚デバイス鍵に基づいて共通秘密を生成するために、処理ユニット６は、メモリ・ユニットから、聴覚デバイス鍵を含む聴覚デバイス証明書を取り出す。

【００６６】

接続要求を受信した後、処理ユニット６は、セッション識別子を乱数または疑似乱数として計算する。処理ユニット６は、メモリ・ユニット６にセッション識別子を記憶する。処理ユニット６は、セッション識別子に基づいて共通秘密を生成し、共通秘密をメモリ・ユニットに記憶する。処理ユニット４は、セッション識別子、共通秘密、聴覚デバイス鍵、および証明書鍵を生成するように構成され得る。したがって、処理ユニット４は、例えば、生成ユニット４２を備える。例えば、処理ユニット６は、聴覚デバイス鍵およびセッション識別子に基づいて共通秘密を生成する。処理ユニット６は、共通秘密ＣＳを、例えば以下の式

ＣＳ＝ｈａｓｈ（ＨＤ＿ＫＥＹ，Ｓ＿ＩＤ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＫＥＹは聴覚デバイス鍵であり、Ｓ＿ＩＤはセッション識別子である。

【００６７】

処理ユニット６は、共通秘密および／または証明書値に対してハッシュ関数を実行することによって証明書鍵を生成し得る。処理ユニット６は、証明書鍵Ｃ＿ＫＥＹを、例えば以下の式

Ｃ＿ＫＥＹ＝ｈａｓｈ（ＣＳ，Ｃ＿ＶＡＬ）

で生成することができる。ここで、ｈａｓｈはハッシュ関数であり、ＣＳは共通秘密であり、Ｃ＿ＶＡＬは証明書値である。証明書値は、予め定義された値または文字列、例えば「ｃｅｒｔｉｆｉｃａｔｅ」であってよい。

【００６８】

処理ユニット６は、生成された証明書鍵を使用して暗号化されたクライアント・デバイ

ス証明書を復号し、クライアント・デバイス証明書の復号されたバージョンを取得する。次いで、処理ユニット６は、クライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出し、クライアント・デバイス識別子を記憶する。聴覚デバイスは、クライアント・デバイス証明書の復号されたバージョンの内容を検証し得る。

【００６９】

１つまたは複数の例示的な聴覚デバイスにおいて、認証メッセージは、クライアント・デバイス・タイプ識別子を、例えば、（暗号化された）クライアント・デバイス証明書の一部として備える。処理ユニット６は、メモリ・ユニット６にクライアント・デバイス・タイプ識別子を記憶するように構成される。例えば、クライアント・デバイス証明書の復号されたバージョンは、クライアント・デバイス・タイプ識別子を含む。例示的な聴覚デバイスおよび／または方法において、認証メッセージは、クライアント・デバイス・タイプ識別子をプレーン・テキストで含む。

【００７０】

認証メッセージは、ユーザ識別子を備え、処理ユニット６は、メモリ・ユニット６にユーザ識別子を記憶するように構成され得る。例えば、聴覚デバイス２は、ユーザ識別子を認証メッセージ中にプレーン・テキストとして、または認証メッセージ中に含まれる暗号化されたクライアント・デバイス証明書の一部として受信する。

【００７１】

聴覚デバイス２は、処理ユニット４によって、接続要求の受信に応答してセッション識別子を含む接続応答を生成するように構成され得る。聴覚デバイス２は、インターフェース８を介して、接続応答を送信するように構成され得る。例えば、聴覚デバイス２は、インターフェース８を介して接続要求を受信し、処理ユニット４を使用して乱数をセッション識別子として生成し、セッション識別子を接続応答に入れ、接続応答をクライアント・デバイス１０に送信する。例えば、インターフェース８は、接続要求を、例えばクライアント・デバイス１０から受信するように構成される。インターフェース８で接続要求を受信した後、インターフェース８は、セッション識別子を乱数または疑似乱数として生成してセッション識別子を接続応答に入れる処理ユニット４に通知する。インターフェース８は、接続応答を送信する。

【００７２】

１つまたは複数の例示的な聴覚デバイスにおいて、聴覚デバイス２は、共通秘密をクライアント・デバイス識別子にリンクするように構成される。例えば、聴覚デバイス２は、リストまたはテーブルにおいて、共通秘密をクライアント・デバイス識別子に関連付けることによって共通秘密をクライアント・デバイス識別子にリンクするように構成される。共通秘密をクライアント・デバイス識別子にリンクすることで、同じクライアント・デバイス１０が聴覚デバイス２に再び接続し、認証メッセージにおいてプレーン・テキストでそのクライアント・デバイス識別子を提供するとき、聴覚デバイス２がメモリ６から共通秘密を取り出し、共通秘密に基づいて直接証明書鍵を導出することを可能にし得る。これは、聴覚デバイス２にある程度の計算および電力効率をもたらし得る。

【００７３】

１つまたは複数の例示的な聴覚デバイスにおいて、聴覚デバイス２は、セッション識別子をメモリ・ユニット６に記憶するように構成される。聴覚デバイス２は、リストまたはテーブルにおいて、セッション識別子およびメモリ・ユニット６内のクライアント識別子を関連付けるなど、セッション識別子をメモリ・ユニット６内のクライアント識別子にリンクするように構成され得る。例えば、処理ユニット４は、セッション識別子とクライアント識別子との間のメモリ関連付けを実行するなど、またテーブルにおいて、共通秘密をクライアント・デバイス識別子に関連付けるなどのために、メモリ・ユニットにおいてセッション識別子およびクライアント識別子をリンクするように構成される。これにより、次の通信またはセッションなどの、後の段階で同じユーザおよびクライアント・デバイス１０の認証を簡素化するという利点がもたらされ得る。

【００７４】
図３Ａは、例示的なクライアント・デバイス証明書１０６を概略的に示す。認証メッセージは、クライアント・デバイス証明書１０６または暗号化されたクライアント・デバイス証明書１０６Ａを含み得る。クライアント・デバイス１０は、クライアント・デバイス証明書１０６を割り当てられ得る。クライアント・デバイス証明書１０６は、例えば、クライアント・デバイス１０を製造するデバイスによって、生成され、クライアント・デバイスに割り当てられる証明書を指す。暗号化されたクライアント・デバイス証明書１０６Ａは、暗号化アルゴリズムおよび証明書鍵を使用してクライアント・デバイス１０によって生成され得る。クライアント・デバイス証明書１０６は、証明書タイプ識別子１３０Ａを備え得る。証明書タイプ識別子１３０Ａは、聴覚デバイス・ファミリ証明書タイプ、聴覚デバイス証明書タイプ、ファームウェア証明書タイプ、研究開発証明書タイプ、クライアント・デバイス証明書タイプなどの、さまざまな証明書タイプのうちの１つの証明書タイプを示し得る。証明書タイプ識別子１３０Ａは、どのようなタイプの証明書を受信し、記憶し、および／または取り出すかを識別するために聴覚デバイス２によって使用され得る。クライアント・デバイス証明書１０６は、クライアント・デバイス証明書１０６のデータ・フォーマット・バージョンを示すバージョン識別子１３２を含むものとしてよい。聴覚デバイス２は、証明書タイプ識別子１３０Ａおよび／またはバージョン識別子１３２を使用して、証明書がどのようなタイプのデータを含むか、および／またはどのようなタイプのデータが証明書のフィールドに入っているかを決定するように構成され得る。例えば、聴覚デバイス２は、証明書タイプ識別子１３０Ａおよび／またはバージョン識別子１３２に基づいて、証明書１０６のどのようなフィールドがデジタル署名１１３Ａを含むか、および／またはデジタル署名１１３Ａを検証するためにどの公開鍵が必要かを決定する。証明書タイプ識別子１３０Ａと公開／秘密鍵ペアとの間に一対一マッピングがあることが想定され得る。クライアント・デバイス証明書１０６は、１つまたは複数の署名デバイス識別子１３６Ａを備え得る。署名デバイス識別子１３６Ａは、クライアント・デバイス証明書１０６に署名したデバイス（製造デバイス、例えば集積回路カード、スマート・カード、ハードウェア・セキュリティ・モジュールなど）を識別する一意の識別子を指す。署名デバイス識別子１３６Ａは、例えば、署名デバイスの媒体アクセス制御（ＭＡＣ）アドレス、シリアル番号を含み得る。署名デバイス識別子１３６Ａは、例えば、聴覚デバイス２が、署名デバイスが例えばブラックリストに載っているかどうかを決定すること、したがってブラックリストに載っている署名デバイスによって署名された証明書を拒絶することを可能にする。クライアント・デバイス証明書１０６は、第１のハードウェア識別子１４８Ａおよび第２のハードウェア識別子１５０などの１つまたは複数のハードウェア識別子を備え得る。ハードウェア識別子１４８Ａ、１５０は、クライアント・デバイスに備えられている無線チップおよび／またはクライアント・デバイスのデジタル・シグナル・プロセッサなどの、クライアント・デバイス１０に備えられているハードウェアを識別することができる。ハードウェア識別子は、ハードウェアの製造時に聴覚デバイスに備えられているハードウェアのレジスタに記憶され得る。ハードウェア識別子は、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組合せを含み得る。

【００７５】
１つまたは複数の例示的なクライアント・デバイス証明書において、クライアント・デバイス証明書１０６は、クライアント・デバイス・タイプ識別子１５６を含む。クライアント・デバイス・タイプ識別子１５６は、クライアント・デバイスが属しているタイプを示し得る。クライアント・デバイス証明書１０６は、クライアント・デバイス識別子１５８を備え得る。クライアント・デバイス証明書は、クライアント・デバイス鍵識別子１５９を備え得る。クライアント・デバイス鍵識別子１５９は、外部パーティとの通信を保護するための鍵材料として使用されるクライアント・デバイス鍵を示し得る。クライアント・デバイス鍵識別子１５９は、どのクライアント・デバイス鍵が、クライアント・デバイス証明書１０６の一部であるかを示し得る。

【００７６】
１つまたは複数の例示的なクライアント・デバイス証明書において、クライアント・デバイス証明書１０６は、クライアント・デバイスのＢｌｕｅｔｏｏｔｈアドレス１６０を含む。
【００７７】
クライアント・デバイス証明書１０６は、デジタル署名１１３Ａを備える。デジタル署名１１３Ａは、署名者の正当性の検証などの、クライアント・デバイス証明書の真正性の立証または検証を可能にする。デジタル署名１１３Ａは、適宜、クライアント・デバイス・フィッティング秘密鍵を使用して製造デバイス１２によって生成される。聴覚デバイス２は、デジタル署名１１３Ａを備えるクライアント・デバイス証明書を受信したとき（すなわち、暗号化されたクライアント・デバイス証明書を含む認証メッセージを受信し、クライアント・デバイス証明書の復号されたバージョン１０６Ｂを取得したとき）にデジタル署名１１３Ａを検証するように構成され得る。デジタル署名１１３Ａは、対応するクライアント・デバイス・フィッティング公開鍵を使用して聴覚デバイス２によって検証可能である。デジタル署名１１３Ａが、申し立てられた公開鍵を使用して検証に成功しなかった場合、聴覚デバイス２は、クライアント・デバイス証明書１０６（認証メッセージ）を破棄し、および／または通常動作を中断することができる。これは、聴覚デバイス２が改竄されたまたは非認証パーティから受信されたクライアント・デバイス証明書１０６（認証メッセージ）を拒絶するという利点をもたらし得る。したがって、聴覚デバイス２との通信は、偽装攻撃、変更攻撃、およびなりすまし攻撃に対してロバストであり得る。
【００７８】
図３Ｂは、例示的な聴覚デバイス証明書１００を概略的に示す。聴覚デバイス証明書１００は、聴覚デバイス識別子１１２、聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子１１４を含む少なくとも１つの聴覚デバイス鍵識別子、および１つまたは複数の聴覚デバイス鍵を備える。聴覚デバイス識別子１１２は、一意のまたは疑似一意の識別子を指すものとしてよい。第１の聴覚デバイス鍵識別子１１４は、聴覚デバイス証明書の第１の聴覚デバイス鍵を示す。例えば、第１の聴覚デバイス鍵識別子１１４は、聴覚デバイス証明書の聴覚デバイス鍵の第１のセット１１５（１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄ）のうちの１つの聴覚デバイス鍵、例えば、第１の一次聴覚デバイス鍵１１５Ａを示すか、または指しているものとしてよい。
【００７９】
聴覚デバイス証明書１００は、適宜、対応する数の異なるクライアント・デバイス／クライアント・デバイス・タイプとの、安全であり、明確に区別できる通信を可能にする聴覚デバイス鍵の、２つ、３つ、または少なくとも４つのセットを備える。
【００８０】
聴覚デバイス証明書１００は、第１の一次聴覚デバイス鍵１１５Ａを含む聴覚デバイス鍵の第１のセット１１５を備える。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄの第１のセット１１５のうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子１１４を含む。聴覚デバイス鍵の第１のセット１１５は、例えば、第１のクライアント・デバイスまたは第１のクライアント・デバイス・タイプへの、および第１のクライアント・デバイスまたは第１のクライアント・デバイス・タイプからの、通信を保護することのみを目的とする第１の一次鍵１１５Ａ、第１の二次鍵１１５Ｂ、第１の三次鍵１１５Ｃ、および第１の四次鍵１１５Ｄを含む。例えば、聴覚デバイス鍵の第１のセット１１５は、第１のクライアント・デバイスによる聴覚デバイス・データの通信を保護するための聴覚デバイス鍵１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄのセットであってよい。
【００８１】
複数の聴覚デバイス鍵は、第２の一次聴覚デバイス鍵１１７Ａ、第２の二次聴覚デバイス鍵１１７Ｂ、第２の三次聴覚デバイス鍵１１７Ｃ、および／または第２の四次聴覚デバイス鍵１１７Ｄを含む聴覚デバイス鍵の第２のセット１１７を含み得る。少なくとも１つ

の聴覚デバイス鍵識別子は、聴覚デバイス鍵１１７Ａ、１１７Ｂ、１１７Ｃ、１１７Ｄの第２のセット１１７のうちの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子１１６を含む。聴覚デバイスは、第１のクライアント・デバイスおよび／または第２のクライアント・デバイスなどの、１つまたは複数のクライアント・デバイスと通信するように構成される。聴覚デバイスが通信するように構成されている各クライアント・デバイスまたはクライアント・デバイス・タイプについて、聴覚デバイス証明書は、特定のクライアント・デバイスまたはクライアント・デバイス・タイプとの安全な通信を可能にするように構成された聴覚デバイス鍵のセット、およびどの聴覚デバイス鍵が聴覚デバイス証明書の一部であるかを示す聴覚デバイス鍵識別子を備える。聴覚デバイス証明書は、第３の一次聴覚デバイス鍵１１９Ａ、第３の二次聴覚デバイス鍵１１９Ｂ、第３の三次聴覚デバイス鍵１１９Ｃ、および／または第３の四次聴覚デバイス鍵１１９Ｄを含む聴覚デバイス鍵の第３のセット１１９を含み得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第３のセット１１９のうちの聴覚デバイス鍵を示す第３の聴覚デバイス鍵識別子１１８を含む。聴覚デバイス証明書１００は、第４の一次聴覚デバイス鍵（図示せず）を含む聴覚デバイス鍵の第４のセットを備え得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第４のセットのうちの聴覚デバイス鍵を示す第４の聴覚デバイス鍵識別子を含む。聴覚デバイス２は、聴覚デバイスに接続されているクライアント・デバイスまたはクライアント・デバイス・タイプに基づいて聴覚デバイス鍵のセットを選択し、聴覚デバイスの選択されたセットに関連付けられている聴覚デバイス鍵識別子に基づいて聴覚デバイス鍵のセットから聴覚デバイス鍵を１つ選択するように構成され得る。

【００８２】

聴覚デバイス証明書１００は、証明書タイプ識別子１３０Ｂを備える。証明書タイプ識別子１３０Ｂは、例えば、聴覚デバイス・ファミリ証明書タイプ、聴覚デバイス証明書タイプ、ファームウェア証明書タイプ、研究開発証明書タイプ、およびクライアント・デバイス証明書タイプなどの、さまざまな証明書タイプのうちから選択された聴覚デバイス証明書であることを示す。証明書タイプ識別子１３０Ｂは、どのようなタイプの証明書を受信し、記憶し、認証し、および／または取り出すかを聴覚デバイス２が識別できるようにするために使用され得る。聴覚デバイス証明書１００は、聴覚デバイス証明書のデータ・フォーマット・バージョンを示すバージョン識別子を含むものとしてよい。聴覚デバイス２は、証明書タイプ識別子１３０Ｂおよび／またはバージョン識別子を使用して、聴覚デバイス証明書１００がどのようなタイプのデータを含むか、どのようなタイプのデータが聴覚デバイス証明書１００のフィールドに入っているかを決定することができる。例えば、聴覚デバイス２は、証明書タイプ識別子１３０Ｂおよび／またはバージョン識別子に基づいて、証明書のどのようなフィールドがデジタル署名１１３Ａを含むか、およびデジタル署名１１３Ａを検証するためにどの公開鍵が必要かを決定し得る。証明書タイプ識別子１３０Ｂと公開／秘密鍵ペアとの間に、デジタル署名１１３Ａを生成するために使用される一対一マッピングがあることが想定され得る。聴覚デバイス証明書１００は、聴覚デバイス証明書１００の長さを、例えば、ビット、バイト単位で示す長さ識別子を含むものとしてよい。

【００８３】

聴覚デバイス証明書１００は、適宜、署名デバイス識別子１３６Ｂを備える。署名デバイス識別子１３６Ｂは、聴覚デバイス証明書１００に署名したデバイス（製造デバイス１２、例えば、製造デバイス１２に含まれる集積回路カード、スマート・カード、ハードウェア・セキュリティ・モジュールなど）を識別する一意の識別子を指す。署名デバイス識別子１３６Ｂは、例えば、署名デバイスの媒体アクセス制御（ＭＡＣ）アドレス、シリアル番号を含み得る。署名デバイス識別子１３６Ｂは、例えば、聴覚デバイス２が、署名デバイスが例えばブラックリストに載っているかどうかを決定すること、したがってブラックリストに載っている署名デバイスによって署名された聴覚デバイス証明書１００を拒絶することを可能にする。

【００８４】

聴覚デバイス証明書１００は、適宜、第１のハードウェア識別子１４８Ｂおよび／または第２のハードウェア識別子（図示せず）を含む１つまたは複数のハードウェア識別子を備える。第１のハードウェア識別子１４８Ｂは、処理ユニット４、聴覚デバイス２に備えられている無線チップ、聴覚デバイス２のデジタル・シグナル・プロセッサなどの、聴覚デバイス２に備えられているハードウェアを識別することができる。第１のハードウェア識別子１４８Ｂは、ハードウェアの製造時に聴覚デバイス２に備えられているハードウェアのレジスタに記憶され得る。第１のハードウェア識別子１４８Ｂは、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組合せを含み得る。聴覚デバイス証明書１００は、第１のハードウェア識別子１４８Ｂ、第２のハードウェア識別子、および／または第３のハードウェア識別子を含み得る。例えば、第１のハードウェア識別子１４８Ｂは、聴覚デバイス２のハードウェア・モジュール（例えば、処理ユニットまたは無線チップ）のレジスタ内に存在する第１の聴覚デバイスに特有の値を与えることができ、第２のハードウェア識別子は、聴覚デバイス２のハードウェア・モジュールのレジスタ内に存在する第２の聴覚デバイスに特有の値を与えることができ、第３のハードウェア識別子は、第３のハードウェア・モジュール識別子（例えば、処理ユニット識別子、ＤＳＰ識別子）を与えることができる。聴覚デバイス２は、第１のハードウェア識別子１４８Ｂを含む聴覚デバイス証明書１００を受信した後に、次いで、記憶されているハードウェア識別子と受信された聴覚デバイス証明書１００に含まれる第１のハードウェア識別子１４８Ｂとを比較することによって聴覚デバイス証明書１００を検証し得る。このようにして、聴覚デバイス２は、受信された聴覚デバイス証明書が聴覚デバイス２を意図したものであるかどうかを判定し、記憶され、受信されたハードウェア識別子が一致しない場合に受信された聴覚デバイス証明書を拒絶し得る。

【００８５】

聴覚デバイス証明書１００は、適宜、クライアント・デバイス・タイプ承認識別子１４４を備える。クライアント・デバイス・タイプは、タブレット製品モデル、カテゴリ、またはタイプ、ＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアント・デバイスのモデル、カテゴリ、またはタイプを含み得る。クライアント・デバイス・タイプ承認識別子１４４は、フィッティング、保守、および／または運用などのために、聴覚デバイス２が通信を承認し得るクライアント・デバイス・タイプの識別子などの、承認されたクライアント・デバイス・タイプの識別子である。クライアント・デバイス・タイプ承認識別子１４４は、例えば、聴覚デバイス２がフィッティングのために許容すべきであるクライアント・デバイスのタイプを示すビット・フィールドである。

【００８６】

聴覚デバイス証明書１００は、適宜、トークン・パラメータ１４６を備える。トークン・パラメータ１４６は、トークンベースの認証が有効化されているかどうかを示す。例えば、トークン・パラメータ１４６が、０に設定されている場合、クライアント・デバイスのトークンベースの認証は、聴覚デバイス２によって有効化されることはなく、聴覚デバイス２は、例えば、クライアント・デバイス・タイプ識別子および／またはクライアント・デバイス識別子（シリアル番号など）の組合せを使用してクライアント・デバイス１０の認証を実行することになる。例えば、トークン・パラメータ１４６が、１に設定されている場合、クライアント・デバイスのトークンベースの認証は、聴覚デバイス２によって有効化されることになる、すなわち、聴覚デバイス２は、（クライアント・デバイス１０から受信されたトークンに基づくなどして）クライアント・デバイス１０を認証する。聴覚デバイス２は、例えばユーザの介入なくクライアント・デバイス１０への接続を受け入れるために使用される受信されたトークン・パラメータ１４６に基づいてセッション特有のトークンも導出し得る。

【００８７】

聴覚デバイス証明書１００は、ハードウェア・プラットフォーム識別子１３８、ソフトウェア・プラットフォーム識別子１４０、および／または証明書タイムスタンプ１４２のうちの１つまたは複数を備える。ハードウェア・プラットフォーム識別子１３８は、動作

している聴覚デバイス・ハードウェア・プラットフォーム、すなわち、聴覚デバイス証明書が使用され得るハードウェア・プラットフォームなどの、ハードウェア・プラットフォームを識別し得る。ソフトウェア・プラットフォーム識別子１４０は、聴覚デバイス証明書が動作するように構成されているソフトウェア・プラットフォームのファミリを識別し得る。証明書タイムスタンプ１４２は、聴覚デバイス証明書１００が生成されたときの時刻を示す製造デバイス１２のタイムスタンプなどの、聴覚デバイス証明書１００の生産または製造のタイムスタンプを指す。証明書タイプスタンプ１４２は、例えば、時、分、日、月、年の形態であるものとしてよい。

【００８８】

聴覚デバイス証明書は、デジタル署名１１３Ｂおよび／またはＭＡＣを備える。デジタル署名１１３Ｂは、署名者の正当性（例えば、署名者が正当な製造デバイスであるかどうか）の検証などの、聴覚デバイス証明書１００の真正性の立証または検証を可能にする。デジタル署名１１３Ｂは、聴覚デバイスの製造時にデバイス・ファミリ秘密鍵を使用して製造デバイス１２によって生成される。次いで、聴覚デバイス２または処理ユニット４は、例えば、デジタル署名１１３Ｂを含む聴覚デバイス証明書１００を受信したとき、デジタル署名１１３Ｂを検証することができる。デジタル署名１１３Ｂは、対応するデバイス・ファミリ公開鍵を使用して聴覚デバイス２によって検証可能である。デジタル署名１１３Ｂが、申し立てられた公開鍵を使用して検証に成功しなかった場合、聴覚デバイスは、聴覚デバイス証明書１００を破棄し、および／または通常動作を中断することができる。

【００８９】

図４は、ログ機能を備える聴覚デバイス２およびクライアント・デバイス１０を伴う例示的な信号図４００を概略的に示している。クライアント・デバイス１０は、フィッティング・デバイス１４を備え得る。聴覚デバイス２は、クライアント・デバイス１０から接続要求またはメッセージ４１１を受信する。クライアント・デバイス１０が、フィッティング・デバイス１４を備えているとき、フィッティング・デバイス１４は、接続要求４１１としてクライアント・デバイス１０によって送信される、接続要求４１０を生成し得る。聴覚デバイス２は、聴覚デバイス識別子１１２および／またはセッション識別子１８０を含む接続応答４１２を生成する。クライアント・デバイス１０が、フィッティング・デバイス１４を備えているとき、フィッティング・デバイス１４は、クライアント・デバイス１０を介して接続応答４１２を受信し得る。クライアント・デバイス１０は、認証メッセージ４２１を生成し、認証メッセージ４２１を聴覚デバイス２に送信する。認証メッセージ４２１は、暗号化されたクライアント・デバイス証明書１０６Ａ、認証鍵識別子１６６、および／または認証タイプ識別子１６８を含む。クライアント・デバイス・タイプ識別子１５６、クライアント・デバイス識別子１５８、ユーザ識別子のうちのどれかが、暗号化されたクライアント・デバイス証明書１０６Ａに含まれ得る。クライアント・デバイス識別子、クライアント・デバイス・タイプ識別子１５６、および／またはユーザ識別子のうちのどれかが、認証メッセージ４２１内に、プレーン・テキストで、例えばクライアント・デバイス証明書１０６の一部として、含まれ得る（図６参照）。聴覚デバイス２は、メモリ・ユニット６に記憶されている聴覚デバイス証明書を使用して認証メッセージ４２１を認証するように構成される。例えば、聴覚デバイス２は、認証メッセージ４２１の内容、発信元、および／または完全性を検証することによって認証メッセージ４２１を認証するように構成される。聴覚デバイス２は、クライアント・デバイス・タイプ識別子に基づいてクライアント・デバイスのタイプを決定する。聴覚デバイス２は、受信された認証鍵識別子１６６の受信された値が、聴覚デバイス証明書１００に含まれる聴覚デバイス鍵識別子（および／または聴覚デバイス２が例えばフラッシュ・メモリに聴覚デバイス鍵識別子として記憶している最新の値）より高いか、または等しいかどうかを検証する。聴覚デバイス２が、受信された認証鍵識別子１６６の受信された値が聴覚デバイス鍵識別子よりも高いか、または等しいと決定した場合に、認証は継続する。そうでなければ、セッションは、即座に打ち切られる（適切なエラー・コードを返す）。これは、聴覚デバイスが失効した／取り消されたクライアント・デバイスと通信することを防ぐ。

【００９０】
聴覚デバイス２は、受信された認証鍵識別子１６６に対応する聴覚デバイス鍵、およびクライアント・デバイス１０への接続応答４１２で送信されたセッション識別子１８０（例えば、１６バイトの乱数）を使用して、例えば証明書鍵が導出可能である共通秘密を計算して、証明書鍵を導出する。
【００９１】
証明書鍵を使用することで、聴覚デバイス２は、暗号化されたクライアント・デバイス証明書１０６Ａを復号する。次いで、聴覚デバイス２は、復号されたクライアント・デバイス証明書１０６Ｂに含まれる証明書タイプ識別子１３０Ａが正しい証明書１０６Ｂに対応していることを検証し得る。次いで、聴覚デバイス２は、プレーン・テキストで受信された認証タイプ識別子１６８が復号された証明書１０６Ｂ中のクライアント・デバイス・タイプ識別子１５６と一致することを検証し得る。次いで、聴覚デバイス２は、プレーン・テキストで受信された認証鍵識別子１６６が、復号された証明書１０６Ｂ中のクライアント・デバイス鍵識別子１５９と一致することを検証することができる。次いで、聴覚デバイス２は、復号された証明書１０６Ｂ中のバージョン識別子１３２が聴覚デバイス２によってサポートされていることを検証し得る。次いで、聴覚デバイス２は、プレーン・テキストで受信された認証タイプ識別子１６８またはクライアント・デバイス・タイプ識別子１５６が記憶されている聴覚デバイス証明書１００のクライアント・デバイス・タイプ承認識別子１４４にリストされていることを検証し得る。次いで、聴覚デバイス２は、プレーン・テキストで受信された認証タイプ識別子１６８または第１のハードウェア識別子１４８Ａ、１５０に関連付けられているクライアント・デバイス・タイプ識別子１５６がブラックリストに載っていないことを検証し得る。署名デバイス識別子１３６Ａは、ブラックリストに載っていないことを検証される。次いで、聴覚デバイス２は、一致する公開鍵を使用してクライアント・デバイス証明書１０６Ｂのデジタル署名１１３Ａを検証し得る。
【００９２】
認証メッセージ４２１の認証および／または検証が成功した後、聴覚デバイス２は、認証応答４２２を、クライアント・デバイス１０に送信することができる。クライアント・デバイス１０は、フィッティング・デバイス１４にそれを転送し得る。
【００９３】
通信チャネルは、この時点で開かれ、安全が確保されている。クライアント・デバイス１０またはクライアント・デバイス１０を介したフィッティング・デバイス１４は、聴覚デバイス・データ４３０を聴覚デバイス２に送信し得る。聴覚デバイス・データ４３０は、例えば、ファームウェア、フィッティング・データ、および／または聴覚デバイス動作パラメータを含む。フィッティング・データは、例えば、聴覚デバイス２がユーザの耳にフィッティングされているときにディスペンサによって使用されるフィッティング・デバイス１４によって生成されるデータであってよい。フィッティング・データは、聴力損失パラメータ、コンプレッサ・パラメータ、フィルタ係数、および／または利得係数を含み得る。聴覚デバイス動作パラメータは、ボリューム・コントロール・パラメータ、モード、および／またはプログラム・コントロール・パラメータを含み得る。ファームウェアは、聴覚デバイス製造者によって提供され、聴覚デバイス２を制御するために聴覚デバイス２上にインストールされるべきコンピュータ・プログラムを指すものとしてよい。ファームウェアは、例えば、聴覚デバイス２の動作および機能をアップグレードするようにインストールされることになる。
【００９４】
図５は、聴覚デバイス２を運用する例示的な方法５００の流れ図を概略的に示す。聴覚デバイス２は、聴覚デバイス２のユーザの聴力損失を補うように構成された処理ユニット４と、メモリ・ユニット６と、インターフェース８とを備える。方法は、インターフェース８を介して、クライアント・デバイス１０から認証メッセージ４２１を受信すること（Ｓ１）と、認証メッセージ４２１からクライアント・デバイス識別子１５８を導出するこ

と（Ｓ２）とを含む。例えば、インターフェース８は、クライアント・デバイス１０から認証メッセージ４２１を受信するように構成され得る。クライアント・デバイス１０は、聴覚デバイス２とのセッションまたは接続を開くために、例えば、フィッティング・データ、聴覚デバイス動作パラメータ、および／またはファームウェア・データを送信するために、認証メッセージ４２１を聴覚デバイス２に送信する。クライアント・デバイス識別子１５８を認証メッセージ４２１から導出すること（Ｓ２）は、認証メッセージ４２１のペイロードを処理することからクライアント・デバイス識別子１５８を取得するなどの、認証メッセージ４２１からクライアント・デバイス識別子１５８を取得することを含み得る。方法は、メモリ・ユニット６にクライアント・デバイス識別子１５８を記憶すること（Ｓ３）を含む。クライアント・デバイス識別子１５８をメモリ・ユニット６に記憶すること（Ｓ３）は、ログ機能に寄与し得る。これは、聴覚デバイスが、聴覚デバイスに関連している１つまたは複数のクライアント・デバイス識別子をログに取るか、または記録することを可能にする。

【００９５】

１つまたは複数の例示的な方法において、認証メッセージ４２１は、暗号化されたクライアント・デバイス証明書１０６Ａを含む。認証メッセージ４２１からクライアント・デバイス識別子１５８を導出すること（Ｓ２）は、暗号化されたクライアント・デバイス証明書１０６Ａを復号することによって暗号化されたクライアント・デバイス証明書１０６Ａの復号されたバージョン１０６Ｂを取得することと、クライアント・デバイス証明書１０６の復号されたバージョン１０６Ｂからクライアント・デバイス識別子１５８を導出することとを含み得る。暗号化されたクライアント・デバイス証明書１９６Ａを復号することは、証明書鍵を使用して暗号化されたクライアント・デバイス証明書１０６Ａを復号することを含み得る。証明書鍵は、共通秘密および／または証明書値に基づくものとしてよい。方法は、聴覚デバイス鍵に基づいて共通秘密を生成することを含み得る。例えば、暗号化されたクライアント・デバイス証明書１０６Ａを復号することは、メモリ・ユニット６から聴覚デバイス証明書１００を取り出すことを含むものとしてよく、聴覚デバイス証明書１００は、１１５Ａなどの聴覚デバイス鍵を含む。例えば、暗号化されたクライアント・デバイス証明書１０６Ａを復号することは、共通秘密に基づいて証明書鍵を生成することを含み得る。方法は、共通秘密を生成することは、聴覚デバイス鍵およびセッション識別子に基づいてもよい。方法は、処理ユニットを使用して共通秘密を生成することと、共通秘密をメモリ・ユニット６に記憶すること（Ｓ４）とを含み得る。方法は、接続要求４１１の受信後にセッション識別子を生成すること（Ｓ５）を含み得る。セッション識別子は、定義された長さの乱数または疑似乱数を含むものとしてよい。共通秘密ＣＳは、例えば以下の式

ＣＳ＝ｈａｓｈ（ＨＤ＿ＫＥＹ，Ｓ＿ＩＤ）

で生成されるものとしてよい。ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＫＥＹは聴覚デバイス鍵であり、Ｓ＿ＩＤはセッション識別子である。

【００９６】

方法は、共通秘密に基づいて証明書鍵を生成することを含み得る。証明書鍵は、秘密および／または証明書値に対してハッシュ関数を実行するによって生成され得る。証明書鍵は、例えば以下の式

Ｃ＿ＫＥＹ＝ｈａｓｈ（ＣＳ，Ｃ＿ＶＡＬ）

で生成されるものとしてよい。ここで、ｈａｓｈはハッシュ関数であり、ＣＳは共通秘密であり、Ｃ＿ＶＡＬは証明書値である。証明書値は、予め定義された値または文字列、例えば「ｃｅｒｔｉｆｉｃａｔｅ」であってよい。

【００９７】

暗号化されているクライアント・デバイス証明書１０６Ａを復号することは、聴覚デバイス２によって生成された証明書鍵を使用することに基づくものとしてよく、その結果、クライアント・デバイス証明書１０６の復号されたバージョン１０６Ｂを取得し得る。次いで、聴覚デバイス２は、クライアント・デバイス証明書１０６の復号されたバージョン

１０６Ｂからクライアント・デバイス識別子１５８を導出し、クライアント・デバイス識別子１５８を記憶する。方法は、クライアント・デバイス証明書１０６の復号されたバージョン１０６Ｂの内容を検証することを含み得る。

【００９８】

１つまたは複数の例示的な方法において、認証メッセージ４２１は、クライアント・デバイス・タイプ識別子１５６を含み、方法は、メモリ・ユニット６にクライアント・デバイス・タイプ識別子１５６を記憶すること（Ｓ６）を含む。

【００９９】

１つまたは複数の例示的な方法において、認証メッセージ４２１は、ユーザ識別子を含み、方法は、メモリ・ユニット６にユーザ識別子を記憶すること（Ｓ７）を含む。

【０１００】

１つまたは複数の例示的な方法において、方法は、接続要求４１１を受信した後にセッション識別子を含む接続応答４１２を生成すること（Ｓ８）と、それを送信すること（Ｓ９）とを含む。方法は、ワイヤレス通信インターフェース、起動ボタン、ユーザ入力の検出、および／またはドッキング・イベントなど、インターフェース８を介して、接続要求４１１を受信することを含み得る。方法は、セッション識別子として使用されるべき乱数または疑似乱数を生成することなど、セッション識別子を生成することを含み得る。方法は、接続応答４１２をインターフェース８を介して例えばクライアント・デバイス１０に送信することを含み得る。

【０１０１】

方法は、セッション識別子に基づいて共通秘密を生成することと、共通秘密をメモリ・ユニット６に記憶すること（Ｓ４）とを含むものとしてよく、共通秘密はクライアント・デバイス識別子１５８にリンクされている。セッション識別子に基づいて共通秘密を生成することは、ハッシュ関数をセッション識別子および聴覚デバイス鍵に適用することに基づくなど、セッション識別子およびハッシュ関数に基づいて共通秘密を生成することを含み得る。共通秘密を生成することは、聴覚デバイス鍵を取り出すことを含む。方法は、共通秘密をクライアント・デバイス識別子１５８にリンクすることを含み得る。例えば、共通秘密をクライアント・デバイス識別子１５８にリンクすることは、共通秘密をメモリ・ユニット６内のリストまたはテーブルの中のクライアント・デバイス識別子１５８に関連付けることなど、共通秘密をクライアント・デバイス識別子１５８に関連付けることを含む。

【０１０２】

１つまたは複数の例示的な方法において、接続応答４１２は、聴覚デバイス２の聴覚デバイス識別子１１２を含み、共通秘密を生成することは、第１の一次聴覚デバイス鍵１１５Ａなど、第１の二次聴覚デバイス鍵１１５Ｂなどの、聴覚デバイス鍵に基づく。例えば、共通秘密を生成することは、メモリ・ユニットに記憶されている聴覚デバイス証明書１００からなど、メモリ・ユニット６から聴覚デバイス鍵を取り出すことを含む。

【０１０３】

方法は、セッション識別子をメモリ・ユニット６に記憶することと、セッション識別子をメモリ・ユニット６内のクライアント識別子１５８にリンクすることとを含み得る。セッション識別子をクライアント・デバイス識別子１５８にリンクすることは、セッション識別子を、メモリ・ユニット６内のリストまたはテーブルなどの中の、クライアント・デバイス識別子１５８に関連付けることを含み得る。

【０１０４】

１つまたは複数の例示的な方法において、方法は、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子および／または共通秘密にリンクすることを含む。例えば、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子および／または共通秘密にリンクすることは、メモリ・ユニット６内の１つまたは複数のリストおよび／またはテーブルなどの中で、ユーザ識別子および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子

および／または共通秘密に関連付けることを含む。
【０１０５】
１つまたは複数の例示的な方法において、方法は、クライアント・デバイス識別子１５８、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子および／または共通秘密にリンクすることを含む。例えば、クライアント・デバイス識別子１５８、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子および／または共通秘密にリンクすることは、メモリ・ユニット内の１つまたは複数のリストおよび／またはテーブルなどの中で、クライアント・デバイス識別子１５８、ユーザ識別子、および／またはクライアント・デバイス・タイプ識別子１５６をセッション識別子および／または共通秘密に関連付けることを含む。
【０１０６】
方法は、メモリ・ユニット６に記憶される聴覚デバイス証明書１００を使用して認証メッセージ４２１を認証すること（Ｓ１０）を含み得る。１つまたは複数の例示的な方法において、認証メッセージ４２１は、認証タイプ識別子、および／または認証鍵識別子を含む。認証タイプ識別子は、認証メッセージ４２１の送信者である、クライアント・デバイス１０のクライアント・デバイス・タイプ識別子１５６を示す。認証鍵識別子は、第１の聴覚デバイス鍵識別子１１４、第２の聴覚デバイス鍵識別子１１６などの、聴覚デバイス鍵識別子を示す。１つまたは複数の例示的な方法において、認証メッセージ４２１は、認証タイプ識別子、および／または認証鍵識別子をプレーン・テキストで含む。メモリ・ユニット６は、そこに記憶される聴覚デバイス証明書１００を有する。聴覚デバイス証明書１００を使用して認証メッセージ４２１を認証すること（Ｓ１０）は、認証タイプ識別子、および／または認証鍵識別子を検証することを含むものとしてよい。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子が聴覚デバイス証明書１００に含まれる第１の聴覚デバイス鍵識別子１１４などの、対応する聴覚デバイス鍵識別子と一致することを検証することを含む。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子が、聴覚デバイス証明書１００に含まれる第１の聴覚デバイス鍵識別子１１４などの、対応する聴覚デバイス鍵識別子の値に等しいか、または高い値を有することを検証することを含む。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証鍵識別子がクライアント・デバイス証明書の復号されたバージョン１０６Ｂに含まれる対応するクライアント・デバイス鍵識別子１５８と一致することを検証することを含む。例えば、認証タイプ識別子および／または認証鍵識別子を検証することは、認証タイプ識別子がクライアント・デバイス証明書の復号されたバージョン１０６Ｂに含まれる対応するクライアント・デバイス・タイプ識別子１５８と一致することを検証することを含む。
【０１０７】
図６は、例示的な信号図４００Ａを示しており、認証メッセージ４２１は、クライアント・デバイス証明書１０６をプレーン・テキストで含む。
【０１０８】
例示的な聴覚デバイスおよび方法は、次の項目に述べられている。
【０１０９】
（項目１）
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、
メモリ・ユニットと、
インターフェースとを備える聴覚デバイスであって、
インターフェースを介して、クライアント・デバイスから認証メッセージを受信し、
認証メッセージからクライアント・デバイス識別子を導出し、
メモリ・ユニットにクライアント・デバイス識別子を記憶するように構成されている、聴覚デバイス。
【０１１０】
（項目２）

認証メッセージは、暗号化されたクライアント・デバイス証明書を含み、認証メッセージからクライアント・デバイス識別子を導出することは、暗号化されたクライアント・デバイス証明書を復号することによって暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得することと、暗号化されたクライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出することとを含む、項目１に記載の聴覚デバイス。

【０１１１】

（項目３）

認証メッセージは、クライアント・デバイス・タイプ識別子を含み、処理ユニットは、メモリ・ユニットにクライアント・デバイス・タイプ識別子を記憶するように構成される、項目１または２に記載の聴覚デバイス。

【０１１２】

（項目４）

認証メッセージは、ユーザ識別子を含み、処理ユニットは、メモリ・ユニットにユーザ識別子を記憶するように構成される、項目１から３のいずれか一項に記載の聴覚デバイス。

【０１１３】

（項目５）

聴覚デバイスは、接続要求を受信したことに応答して処理ユニットによってセッション識別子を含む接続応答を生成し、インターフェースを介して接続応答を送信するように構成される、項目１から４のいずれか一項に記載の聴覚デバイス。

【０１１４】

（項目６）

聴覚デバイスは、処理ユニットによって、セッション識別子に基づいて共通秘密を生成し、共通秘密をメモリ・ユニットに記憶し、共通秘密をクライアント・デバイス識別子にリンクするように構成される、項目５に記載の聴覚デバイス。

【０１１５】

（項目７）

共通秘密をクライアント・デバイス識別子にリンクすることは、テーブルにおいて共通秘密をクライアント・デバイス識別子に関連付けることを含む項目６に記載の聴覚デバイス。

【０１１６】

（項目８）

聴覚デバイスは、聴覚デバイス鍵に基づいて共通秘密を生成するように構成される、項目６または７に記載の聴覚デバイス。

【０１１７】

（項目９）

聴覚デバイスは、セッション識別子をメモリ・ユニットに記憶するように構成され、セッション識別子は、メモリ・ユニット内のクライアント識別子にリンクされる、項目５から８のいずれか一項に記載の聴覚デバイス。

【０１１８】

（項目１０）

聴覚デバイスは、メモリ・ユニットに記憶されている聴覚デバイス証明書を使用して認証メッセージを認証するように構成される、項目１から９のいずれか一項に記載の聴覚デバイス。

【０１１９】

（項目１１）

聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、メモリ・ユニットと、インターフェースとを備える聴覚デバイスを運用する方法であって、

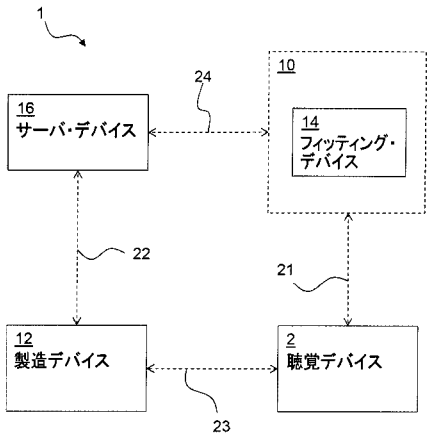
インターフェースを介して、クライアント・デバイスから認証メッセージを受信するス

テップと、
認証メッセージからクライアント・デバイス識別子を導出するステップと、
メモリ・ユニットにクライアント・デバイス識別子を記憶するステップとを含む方法。
【０１２０】
（項目１２）
認証メッセージは、暗号化されたクライアント・デバイス証明書を含み、認証メッセージからクライアント・デバイス識別子を導出するステップは、暗号化されたクライアント・デバイス証明書を復号することによって暗号化されたクライアント・デバイス証明書の復号されたバージョンを取得するステップと、クライアント・デバイス証明書の復号されたバージョンからクライアント・デバイス識別子を導出するステップとを含む、項目１１に記載の方法。
【０１２１】
（項目１３）
認証メッセージは、クライアント・デバイス・タイプ識別子を含み、方法は、メモリ・ユニットにクライアント・デバイス・タイプ識別子を記憶するステップを含む、項目１１または１２に記載の方法。
【０１２２】
（項目１４）
認証メッセージは、ユーザ識別子を含み、方法は、メモリ・ユニットにユーザ識別子を記憶するステップを含む、項目１１から１３のいずれか一項に記載の方法。
【０１２３】
（項目１５）
方法は、セッション識別子を生成するステップと、接続要求を受信した後にセッション識別子を含む接続応答を送信するステップとを含む項目１１から１４のいずれか一項に記載の方法。
【０１２４】
（項目１６）
方法は、セッション識別子に基づいて共通秘密を生成するステップと、共通秘密をメモリ・ユニットに記憶するステップと、共通秘密をクライアント・デバイス識別子にリンクするステップとを含む、項目１５に記載の方法。
【０１２５】
（項目１７）
接続応答は、聴覚デバイスの聴覚デバイス識別子を含み、共通秘密を生成するステップは、聴覚デバイス識別子に基づく、項目１５または１６に記載の方法。
【０１２６】
（項目１８）
方法は、セッション識別子をメモリ・ユニットに記憶するステップと、セッション識別子をメモリ・ユニット内のクライアント識別子にリンクするステップとを含む、項目１５から１７のいずれか一項に記載の方法。
【０１２７】
（項目１９）
方法は、メモリ・ユニットに記憶される聴覚デバイス証明書を使用して認証メッセージを認証するステップを含む、項目１１から１８のいずれか一項に記載の方法。
【０１２８】
「第１の」、「第２の」、および同様の言い回しの使用は、特定の順序を意味しないが、それらは、個別の要素を識別するために含まれている。さらに、第１の、第２の、などの言い回しの使用は、順序、または重要度を表さず、むしろ、第１の、第２の、などは、要素を互いに区別するために使用される。第１および第２という単語は、ここで、および別のところで、標識付けのみを目的として使用されており、特定の空間的または時間的順序付けを表すことを意図されていないことに留意されたい。さらに、第１の要素の標識付

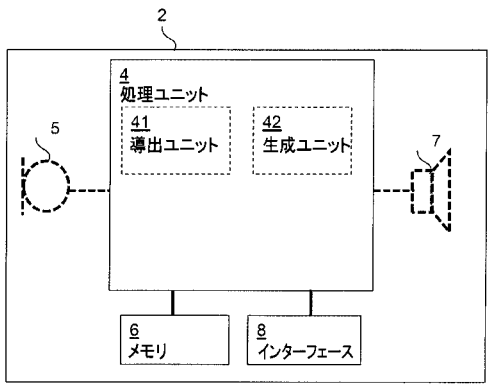
けは、第２の要素の存在を意味しない。
【０１２９】
特定の特徴が示され説明されているが、それらは特許請求の範囲に記載された発明を制限することを意図されていないことは理解され、当業者に対して、さまざまな変更および修正が特許請求の範囲に記載された発明の精神および範囲から逸脱することなくなされ得ることが明らかにされる。したがって、本明細書および図面は、限定ではなく、例示することを目的としているものとみなすべきである。特許請求の範囲に記載された発明は、すべての代替形態、修正形態、および均等形態を対象とすることが意図されている。
【符号の説明】
【０１３０】
２：聴覚デバイス
４：処理ユニット
５：マイクロフォン
６：メモリ・ユニット
７：レシーバ
８：インターフェース
１０：クライアント・デバイス
１２：製造デバイス
１４：フィッティング・デバイス
１６：サーバ・デバイス
２１：クライアント・デバイスと聴覚デバイスとの間の通信リンク
２２：サーバ・デバイスと製造デバイスとの間の通信リンク
２３：聴覚デバイスと製造デバイスとの間の通信リンク
２４：サーバ・デバイスとクライアント・デバイス／フィッティング・デバイスとの間の通信リンク
１００：聴覚デバイス証明書
１００Ａ：暗号化された聴覚デバイス証明書
１００Ｂ：暗号化された聴覚デバイス証明書の復号されたバージョン
１０６：クライアント・デバイス証明書
１０６Ａ：暗号化されたクライアント・デバイス証明書
１０６Ｂ：暗号化されたクライアント・デバイス証明書の復号されたバージョン
１１２：聴覚デバイス識別子
１１３Ａ：クライアント・デバイス証明書に含まれるデジタル署名
１１３Ｂ：聴覚デバイス証明書に含まれるデジタル署名
１１４：第１の聴覚デバイス鍵識別子
１１５：聴覚デバイス鍵の第１のセット
１１５Ａ：第１の一次聴覚デバイス鍵
１１５Ｂ：第１の二次聴覚デバイス鍵
１１５Ｃ：第１の三次聴覚デバイス鍵
１１５Ｄ：第１の四次聴覚デバイス鍵
１１６：第２の聴覚デバイス鍵識別子
１１７：聴覚デバイス鍵の第２のセット
１１７Ａ：第２の一次聴覚デバイス鍵
１１７Ｂ：第２の二次聴覚デバイス鍵
１１７Ｃ：第２の三次聴覚デバイス鍵
１１７Ｄ：第２の四次聴覚デバイス鍵
１３０Ａ：クライアント・デバイス証明書に含まれる証明書タイプ識別子
１３０Ｂ：聴覚デバイス証明書に含まれる証明書タイプ識別子
１３２：バージョン識別子
１３４：長さ識別子

１３６Ａ：クライアント・デバイス証明書に含まれる署名デバイス識別子
１３６Ｂ：聴覚デバイス証明書に含まれる署名デバイス識別子
１３８：ハードウェア・プラットフォーム識別子
１４０：ソフトウェア・プラットフォーム識別子
１４２：証明書タイムスタンプ
１４４：クライアント・デバイス・タイプ承認識別子
１４６：トークン・パラメータ
１４８Ａ：クライアント・デバイス証明書に含まれる第１のハードウェア識別子
１４８Ｂ：聴覚デバイス証明書に含まれる第１のハードウェア識別子
１５０：クライアント・デバイス証明書に含まれる第２のハードウェア識別子
１５６：クライアント・デバイス・タイプ識別子
１５８：クライアント・デバイス識別子
１５９：クライアント・デバイス鍵識別子
１６０：Ｂｌｕｅｔｏｏｔｈアドレス
１６６：認証鍵識別子
１６８：認証タイプ識別子
１８０：セッション識別子
４００、４００Ａ：信号図
４１０：フィッティング・デバイスからの接続要求
４１１：クライアント・デバイスからの接続要求
４１２：接続応答
４２１：認証メッセージ
４２２：認証応答
４３０：聴覚デバイス・データ
５００：方法

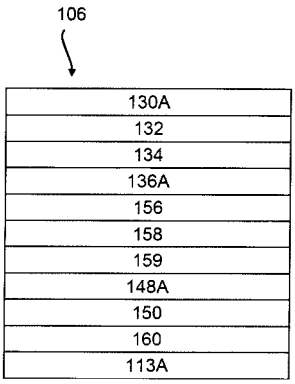
【図１】



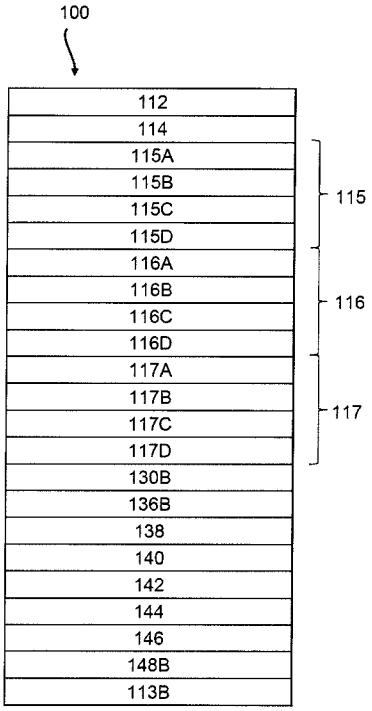
【図２】



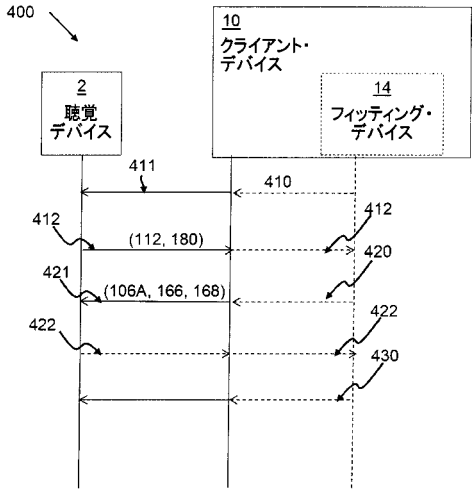
【図３Ａ】



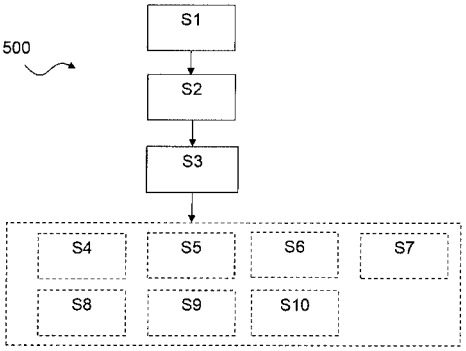
【図３Ｂ】


100
112
114
115A
115B
115C
115D
116A
116B
116C
116D
117A
117B
117C
117D
130B
136B
138
140
142
144
146
148B
113B
115
116
117

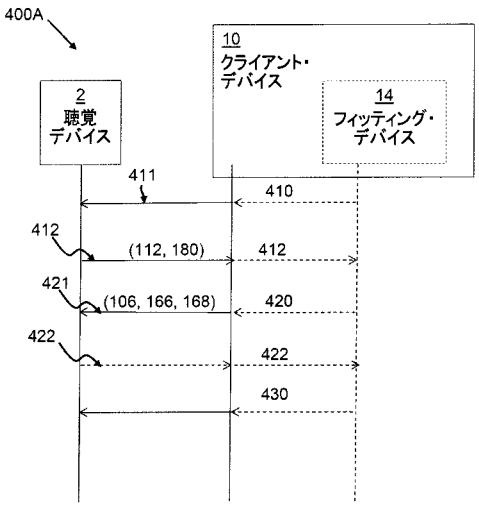
【図４】


400
10
クライアント・
デバイス
2
聴覚
デバイス
14
フィッティング・
デバイス
411
410
412
(112, 180)
412
420
421
(106A, 166, 168)
422
422
430

【図５】


500
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10

【図６】


400A
10
クライアント・
デバイス
2
聴覚
デバイス
14
フィッティング・
デバイス
411
410
412
(112, 180)
412
421
(106, 166, 168)
420
422
422
430

フロントページの続き

(72)発明者　ヴェネルボー　アラン　ムンク
デンマーク　２５００　バルビュー　レンボー　アリ　４

Ｆターム(参考) 5J104 AA09 AA16 AA34 EA04 EA05 EA18 LA02 LA05 LA06 NA02
NA12 NA37

【外国語明細書】
2017017686000001.pdf
2017017686000002.pdf
2017017686000003.pdf
2017017686000004.pdf